DECEPT

DEtection and Handling of CybEr-Physical ATtacks

Programm / Ausschreibung	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 7. Ausschreibung (2018)	**Status**	abgeschlossen
Projektstart	01.02.2020	**Projektende**	31.01.2023
Zeitraum	2020 - 2023	**Projektlaufzeit**	36 Monate
Keywords	anomaly detection, log data analysis, intrusion detection, machine learning, cyber-physical systems		

Projektbeschreibung

Es gibt zwar zahlreiche verhaltensbasierte Anomalieerkennungsansätze für die Sicherheit der "klassischen" Büro-IT von Unternehmen, sie sind jedoch nicht ohne weiteres auf andere Domänen anwendbar, z.B. eingebettete Systeme und IoT. Sie sind normalerweise für bestimmte Zwecke stark optimiert, eng an domänenspezifische Technologien gebunden und basieren auf einer bestimmten Syntax der untersuchten Daten oder Ereignisse. DECEPT stellt einen allgemein anwendbaren domänenübergreifenden Ansatz zur Erkennung von Anomalien bereit, der unstrukturierte Textereignisdaten überwacht (d.h. protokollierte Daten jeder Form, Codierung, Größe oder Häufigkeit) und ein nicht-überwachtes selbstlernendes Verfahren implementiert, das Anwendungen verschiedener unabhängiger Domänen unterstützt. Um die allgemeine Anwendbarkeit zu betonen, wird ein Parser-Generator entwickelt, der das unbeaufsichtigte Selbstlernen anwendet, um ein Modell des normalen Systemverhaltens auf Basis der beobachteten Systemereignisse zu erstellen, das dann zur Erkennung von Anomalien verwendet werden kann, die sich in Abweichungen von dieser Basislinie manifestieren. Darüber hinaus wird ein Konzept zur nicht-überwachten Anomalieerkennung entwickelt, implementiert und validiert, das maschinelle Lerntechniken, Korrelationsregeln, Zeitreihenanalyse und statistische Regeln anwendet, die automatisch generiert und anschließend mit einem intelligenten Regelgenerator und Evaluator ausgewertet werden. Die allgemeine und domänenübergreifende Anwendbarkeit von DECEPT wird in den Bereichen (i) IT-Sicherheit in Unternehmen (Enterpise IT) und (ii) Embedded Systems / IoT-Sicherheit demonstriert. Die konkreten Proof-of-Concepts sind dabei Anomalieerkennung in Web Server Umgebungen und IT-unterstützter Gebäudesicherheit. Im Hinblick auf die DSGVO werden technische Entwicklungen von einem Rechtsexperten überwacht, um die spätere potenzielle kommerzielle Nutzung von DECEPT zu unterstützen.

Abstract

While there exist numerous behavior-based anomaly detection approaches for enterprise-IT security, they are not easily applicable to other domains, e.g. embedded systems and IoT. They are usually highly optimized for specific purposes, are tightly bound to domain-specific technologies and rely on a specific syntax of investigated data or events. DECEPT will provide a generally applicable cross-domain anomaly detection approach, that moni-tors unstructured textual event data (i.e., log data of any form, encoding, size or frequency), and implement un-supervised self-learning, which supports applications in different independent domains. To emphasize general applicability, a parser generator will be developed that

applies unsupervised self-learning to establish a model of normal system behaviour on top of observed system events, which then can be leveraged to detect anomalies that manifest in deviations from that baseline. Furthermore, a concept for un-supervised anomaly detection will be designed, implemented and validated that applies machine learning techniques, correlation rules, time series analysis and statistical rules that will be automatically generated and afterwards evaluated with a smart rule gen-erator and evaluator. DECEPT’s general and cross-domain applicability will be demonstrated in the domains of (i) Enterprise IT security and (ii) Embedded Systems/IoT security. Concrete proof of concepts to be realized are anomaly detection for Web-server landscape security and IT-supported facility security. In light of the GDPR, technical developments will be supervised by a legal expert to aid the later potential commercial exploitation of DECEPT.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- PKE Holding AG
- Huemer iT-Solution Ges.m.b.H.