DEPS

Dependable Production Environments with Software Security

Programm / Ausschreibung	COMET, COMET-Modul, COMET-Modul, 2. Ausschreibung	**Status**	laufend
Projektstart	01.01.2022	**Projektende**	31.12.2026
Zeitraum	2022 - 2026	**Projektlaufzeit**	60 Monate
Keywords	Software Protection, Software-Hardware Binding, Physically Unclonable Functions; Software Diversity, Language based Security		

Projektbeschreibung

Unbefugtes Reverse Engineering im industriellen Maßstab stellt eine große Bedrohung für unsere wissensbasierten Volkswirtschaften und Gesellschaften dar. Diese Bedrohung zieht sich durch mehrere Industriesegmente, da eingebettete Systeme, Maschinen, Roboter und ganze Produktionslinien betroffen sind, die zunehmend wissensintensive integrierte Software zur Ausführung, Steuerung oder Analyse verwenden. Die fortschreitende digitale Transformation durch Digitalisierung und KI wird diese Bedrohung für die europäische und heimische wirtschaftliche Wertschöpfung durch wissensintensive Innovationen in der Industrie und anderen Sektoren noch weiter verstärken. Besonders deutlich wird diese Bedrohung in den Anwendungsbereichen des SCCH mit den Schwerpunkten Software und Data Science. Das Spektrum der Anwendungen ist breit und reicht von der smarten Produktion über die Fernsteuerung von IoT-vernetzten Maschinen auf Baustellen, den Maschinenbau mit integrierten KI-Komponenten bis hin zu medizinischen Geräten, die mit anspruchsvollen Bildanalysefunktionen ausgestattet sind. Die Motivation, sich diesem Thema zu widmen, geht daher mit der Notwendigkeit einher, eine Lücke in der Positionierung des SCCH als Forschungszentrum für Software und AI-System Engineering zu schließen.

Das Ziel von DEPS ist es, diese Herausforderung zu meistern, indem es einen innovativen Ansatz verfolgt, bestimmte Instanzen von Software an bestimmte Instanzen von Hardware auf nicht kopierbare Weise zu binden, um unautorisiertes Reverse Engineering zu verhindern. Zu diesem Zweck strebt DEPS die Kombination von zwei bisher getrennten Forschungsrichtungen an - Software-Diversität und physikalisch unkopierbare Funktionen. Die daraus resultierende Kombination eröffnet eine neue Forschungsrichtung: den Schutz industrieller Produktionssysteme vor unautorisiertem Reverse Engineering.

Der Projektumfang von DEPS erfordert umfangreiche Grundlagenforschung in den beiden getrennten Bereichen und deren anschließende Kombination. Die daraus resultierende gemeinsame Forschungsrichtung birgt großes Potenzial für kostenneutralen und effektiven IP Schutz. Der Nutzen ist zweifach: 1.) für die Gesellschaft die Sicherung von Unternehmen und damit von Arbeitsplätzen; und 2.) für Unternehmen die Sicherung von Gewinnen und die Erhaltung eines Vorsprungs in einer zunehmend wettbewerbsorientierten Welt.

Die neue Forschungsrichtung, die DEPS anstrebt, wird von einem Konsortium wissenschaftlicher Partner mit komplementärer Expertise vorangetrieben, die sich in ihren jeweiligen Bereichen ausgewiesen haben. Ergänzt werden sie durch

Industriepartner aus den betroffenen Anwendungsbereichen der Fertigung, Robotik und eingebetteten Systeme.

Abstract

Unauthorized reverse engineering on an industrial scale poses a major threat to our knowledge-based economies and societies. This threat emerges across various industry segments by affecting embedded systems, machines, robots, and entire production plants, which are increasingly deployed with know-how-intensive built-in software for execution, control, or analysis. The ongoing digital transformation and AI will further increase unauthorized reverse engineering’s negative impact to European and domestic economic value creation through knowledge-intensive innovations in industry and other sectors of the economy. Unauthorized reverse engineering becomes particularly pressing in the application areas of SCCH's overall research agenda with focus on software and data science. The spectrum of applications is broad and includes smart production, remote control of IoT interconnected machines at construction sites, mechanical engineering with integrated AI components, or medical devices equipped with sophisticated image analysis capabilities. The motivation to prevent industrial-scale reverse engineering therefore parallels the need to fill a gap in the positioning of SCCH as research center for software and AI systems engineering focusing on the development cycles of modeling, designing, engineering, quality assurance, and deploying know-how intensive software systems. A side-effect of this application therefore is to significantly strengthen the deployment aspect, and thus SCCH’s overall software and AI system engineering orientation.
The goal of DEPS is to address unauthorized reverse engineering by pioneering a way to bind specific instances of software to specific instances of hardware in an unclonable manner. To this end, DEPS plans to combine two hitherto separate research directions—software diversity and physically-unclonable functions. The resulting combination breaks new ground and establishes a new research direction: industrial production systems protection against unauthorized reverse engineering. The scope of DEPS requires extensive basic research in the two separate areas, as well as their subsequent combination. The resulting joint research direction holds tremendous potential and intellectual merit for cost-neutral, effective, and compositional security. In addition, DEPS seeks to provide comprehensive protection through protection of embedded machine-learned models. The expected broader impact is two-fold: (i) society at large, and (ii) companies. Societal benefits include the protection of companies, and thus their jobs, in Austria. Company benefits include safeguarding of earnings and maintaining an edge in an increasingly competitive world.
The new research direction of DEPS is driven by a consortium of scientific partners having relevant expertise and standing in their respective fields, complemented by industrial partners from impacted application areas in manufacturing, robotics and embedded systems.

Projektkoordinator

- Software Competence Center Hagenberg GmbH

Projektpartner

- Universität der Bundeswehr München
- PwC Wirtschaftsprüfungs- und Steuerberatungsgesellschaft mbH
- framag Industrieanlagenbau GmbH
- FH OÖ Forschungs & Entwicklungs GmbH
- Universität Linz
- Katholieke Universiteit Leuven
- Symflower GmbH

- Plasser & Theurer, Export von Bahnbaumaschinen, Gesellschaft m.b.H.
- SIGMATEK GmbH & Co KG
- EPFL École Polytechnique Fédérale de Lausanne School of Computer and Communication Sciences (IC)