Sicher und souverän: Neues Forschungsprojekt “HEP” entwickelt frei verfügbare Werkzeuge zur Verifikation quelloffener Prozessordesigns

Frankfurt (Oder). Vertrauenswürdigkeit und Sicherheit spielen in der Elektronik eine wichtige Rolle und werden umso bedeutender, je mehr Bereiche des Alltags von der Digitalisierung und Automatisierung beeinflusst werden – sei es die Fahrt im Auto oder die Arbeit im smarten Home Office. Doch wie können diese Aspekte in den Fokus gerückt werden, wenn die einzelnen Bauteile von verschiedensten Herstellern entlang einer globalen Wertschöpfungskette stammen?

Um hierauf Antworten zu finden, hat das Bundesministerium für Bildung und Forschung (BMBF) die Förderinitiative „Vertrauenswürdige Elektronik (ZEUS)“ ins Leben gerufen. Durch die Erforschung, Entwicklung und Anwendung von vertrauenswürdiger Elektronik soll ein Beitrag zur technischen Souveränität in Deutschland und Europa geleistet werden. Um dieses Vorhaben zu unterstützen, beschäftigt sich ein Projektkonsortium um das Leibniz-Institut für innovative Mikroelektronik (IHP) mit Open-Source-Ansätzen für den Entwurf von Computerchips: Das am 1. März 2021 offiziell gestartete Projekt HEP hat zum Ziel, wesentliche Teile der Wertschöpfungskette von sicherheitsrelevanten Chips durch quelloffene Technologien zu realisieren.

Die nächste Hardware-Generation

Im Zentrum des Projekts HEP stehen RISC-V-Prozessoren. RISC-V ist eine neue, offene und freie Befehlssatzarchitektur, die beschreibt, wie der Prozessor genutzt werden kann. RISC-V gilt als vielversprechender quelloffener Standard für viele Einsatzbereiche. Ziel des Projekts ist die Entwicklung eines gehärteten, formal verifizierten RISC-V Prozessors, der kryptographische Operationen mit speziellen Hardwarestrukturen beschleunigen kann.

Die Härtung des Chips zielt darauf ab, möglichst wenige Schwachstellen für physikalische Angriffe auf das System zu bieten. Die Modifizierbarkeit eines verifizierten RISC-V-Prozessors bietet das Potential, sichere Anwendungen für das Internet der Dinge zu ermöglichen und z.B. in der Automobilbranche einen neuen Standard zu etablieren. Deshalb sollen im Projekt auch Erweiterungen für quelloffene Werkzeuge zum Schaltungsentwurf – sogenannte EDA Tools – entwickelt und implementiert werden, die Härtungsmaßnahmen automatisiert in die Schaltungen integrieren. Außerdem soll untersucht werden, wie sich Hardware-Trojaner vom Design bis hin zur Fertigung einfügen lassen und welche Schutzmaßnahmen gegen solche Angriffe möglich sind.

Das Leibniz-Institut für innovative Mikroelektronik (IHP) fokussiert sich in dem Projekt auf das physikalische Design von RISC-V Prozessoren. Ziel der abteilungsübergreifenden Forschungsaktivitäten ist dabei die zweckmäßige Verbindung von Entwurfs-Verifikation und selektiver Härtung des Systems, um so „einen großen Schritt in Richtung Designautomation hochkritischer Systeme im industriellen Umfeld“ zu gehen, wie Dr.-Ing. Markus Ulbricht, Leiter der Fault Tolerant Computing Gruppe des IHP, erläutert.

Industrial Liaison Group verfolgt Weiterentwicklung – auch in kleinen und mittleren Unternehmen

Der Demonstrator, an dem das Projektkonsortium arbeitet, soll im Anschluss in der industriellen Praxis eingesetzt werden. Hierzu wird eine Industrial Liaison Group gegründet, in der die Projektpartner die industrienahe Weiterentwicklung der Ergebnisse verfolgen. Neben dem Ausbau der Kompetenzen für IT-Hardware in der Automobilindustrie und im Internet der Dinge hat das Projekt HEP ebenso zum Ziel, kleine und mittlere Unternehmen zu unterstützen: Quelloffene Prozessoren gestalten nicht nur den Markteinstieg einfacher, sondern sorgen zudem für diversifizierte Wertschöpfungs- und Lieferketten, wodurch Abhängigkeiten reduziert und die Wettbewerbsfähigkeit gestärkt werden.

Das Projekt HEP wird vom Leibniz-Institut für innovative Mikroelektronik (IHP) geleitet. Zu den Partnern gehören zudem:

- IAV GmbH Ingenieursgesellschaft Auto und Verkehr
- Elektrobit Automotive GmbH
- Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI)
- Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
- Hochschule RheinMain, Forschungsschwerpunkt „Smarte Systeme für Mensch und Technik“ (SSMT)
- Ruhr-Universität Bochum, Lehrstuhl für Security Engineering
- Technische Universität Berlin, Department Security in Telecommunications

Als assoziierte Partner sind die CARIAD SE (A Volkswagen Group Company), die HENSOLDT Cyber GmbH, die Hyperstone GmbH, die Robert Bosch GmbH und die Swissbit

Germany AG dabei. Das Bundesministerium für Bildung und Forschung (BMBF) finanziert das Projekt HEP mit rund 3,64 Millionen Euro über einen Zeitraum von drei Jahren.