idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, DFKI
Andrea Fink

02/11/2025
http://idw-online.de/en/news847273

Research projects
Information technology, Mathematics
transregional, national

Schutz vor Cyberangriffen: Projekt setzt mit formaler Verifikation und Flexibilität neue Maßstäbe in der IT-Sicherheit

Cyber-Angriffe auf Unternehmen und öffentliche Einrichtungen nehmen weltweit drastisch zu. Das von der Cyberagentur geförderte Projekt PROTECT entwickelt Lösungen, um IT-Systeme widerstandsfähiger gegen diese Bedrohungen zu machen. Koordiniert vom Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) und in Zusammenarbeit mit führenden Partnern aus Industrie und Forschung verfolgt das Projekt ein klares Ziel: Mit innovativen Methoden der formalen Verifikation soll die IT-Sicherheit auf ein neues Niveau gehoben und das Vertrauen in digitale Systeme nachhaltig gestärkt werden.

Während bisherige Projekte auf einen monolithischen Ansatz mit einer vorgegebenen Methode (top-down) setzten, verfolgt PROTECT (Proving Next Generation Secure Systems) einen Bottom-up-Ansatz. Das bedeutet: Statt Methoden und Werkzeuge starr vorzugeben, entwickelt das Projekt eine flexible Kombination verschiedener formaler Methoden und Werkzeuge. Diese sollen sich nahtlos in bestehende IT-Architekturen integrieren lassen. So können Anwendende je nach Bedarf einzelne Sicherheitskomponenten auswählen und bestehende Systeme gezielt mit einem hohen Maß an Sicherheit erweitern.

„Mit PROTECT setzen wir zukunftsfähige Standards für eine sichere und nachhaltige digitale Infrastruktur. Der innovative Bottom-up-Ansatz ermöglicht die Entwicklung maßgeschneiderter Sicherheitslösungen, die gezielt auf die spezifischen Anforderungen unterschiedlicher IT-Systeme zugeschnitten werden können. Um dies zu erreichen, arbeiten wir mit führenden Partnern aus Wissenschaft und Industrie zusammen“, erklärt Prof. Dr. Christoph Lüth, Projektleiter am DFKI in Bremen.

Zugang für alle: Offene Standards und Open Source

Ein weiteres zentrales Merkmal von PROTECT ist das Bekenntnis zu Open Source und Open Science. Alle entwickelten Werkzeuge und Methoden werden, soweit möglich, als Open-Source-Software zur Verfügung gestellt, um eine breite Nutzung und Anpassung durch die wissenschaftliche Gemeinschaft, die Industrie und andere Interessierte zu ermöglichen. Gleichzeitig sollen die wissenschaftlichen Ergebnisse des Projekts durch Open Access-Publikationen der Öffentlichkeit zugänglich gemacht werden.

Ein Referenzsystem auf Basis von RISC-V

In PROTECT entwickeln die Projektpartner ein Referenzsystem auf Basis eines RISC-V-Prozessors. RISC-V ist eine offene, lizenzfreie Prozessorarchitektur, die besonders flexible und anpassbare Hardwarelösungen für sicherheitskritische Anwendungen ermöglicht. Diese Offenheit erlaubt die Entwicklung maßgeschneiderter, kostengünstiger Lösungen, die speziell auf die Sicherheitsanforderungen von Systemen zugeschnitten sind. Anhand des Referenzsystems werden fortschrittliche hardwarebasierte Sicherheitsmechanismen entwickelt, die vor hochspezialisierten Angriffen wie Seitenkanalangriffen durch transienten Code schützen. Eine weitere Innovation ist die

Nutzung eines digitalen Zwillings (virtueller Prototyp) des Referenzsystems, um mögliche Sicherheitslücken frühzeitig zu erkennen und zu beheben.

Mehr Sicherheit für Unternehmen und digitale Infrastrukturen

Die Ergebnisse von PROTECT haben das Potenzial, die IT-Sicherheit von Unternehmen und öffentlichen Einrichtungen deutlich zu verbessern und neue Standards für die Entwicklung cybersicherer Hard- und Software zu setzen. Insbesondere kleine und mittelständische Unternehmen profitieren von den Open-Source-Lösungen, die einen einfachen Zugang zu fortschrittlichen Sicherheitsfunktionen ermöglichen. Langfristig wird PROTECT dazu beitragen, das Vertrauen in digitale Infrastrukturen zu stärken und IT-Sicherheit auf breiter Basis zu fördern.

Das PROTECT-Konsortium

Das Projekt wird vom DFKI Forschungsbereich Cyber-Physical Systems in Bremen koordiniert. Weitere Partner sind die RWTH Aachen, Cryspen SARL (Paris, Frankreich), die Gesellschaft für Informatik e.V. (Berlin/Bonn), die Technische Universität Kaiserslautern, die LUBIS EDA GmbH (Kaiserslautern) und die Universität zu Lübeck.

PROTECT wird vom 20.12.2024 bis zum 19.12.2028 von der Cyberagentur im Rahmen des Programms „Ökosystem vertrauenswürdige IT – Beweisbare Cybersicherheit“ (ÖvIT) in vier Jahrestranchen mit einer Gesamtsumme von rund 9,15 Millionen Euro (zzgl. Umsatzsteuer) als Forschungsauftrag finanziert.

Pressekontakt:
Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)
Team Communications & Media
Telefon: +49 421 17845 4180
Mail: communications-hb@dfki.de

contact for scientific information:

DFKI-Kontakt:
Prof. Dr. Christoph Lüth
Cyber-Physical Systems
Telefon: +49 421 218 59830
Mail: christoph.lueth@dfki.de

URL for press release: https://cloud.dfki.de/owncloud/index.php/s/H7QqReJz5fJNkzc Ein Symbolbild steht in der DFKI-Cloud zum Download bereit. Dieses können Sie unter Angabe des Copyrights „Treecha/stock.adobe.com“ für die Berichterstattung zum Projekt PROTECT verwenden.

Neues IT-Sicherheitsprojekt PROTECT – Widerstandsfähigkeit gegen Cyberangriffe stärken
Treecha/stock.adobe.com
Treecha/stock.adobe.com