Bundesministerium
für Bildung
und Forschung

Presse-
mitteilung

HAUSANSCHRIFT Hannoversche Straße 28-30, 10115 Berlin
POSTANSCHRIFT 11055 Berlin

TEL 030/18 57-50 50
FAX 030/18 57-55 51
E-MAIL presse@bmbf.bund.de
HOMEPAGE www.bmbf.de

09. Juli 2007
148/2007

„Verified in Germany“ wird Qualitätsmerkmal deutscher Software

Forschungsministerium fördert weltweit führendes Innovationsprojekt

Softwarefehler verursachen in Europa jährlich einen wirtschaftlichen Schaden von weit über 100 Milliarden Euro. Weil bei der Entwicklung von Software die Anforderungen oft falsch eingeschätzt werden und die existierende Technologie der Fehlersuche sehr aufwändig ist, wenden Hersteller heute 70–80 Prozent ihrer Arbeit für das Entfernen von Softwarefehlern auf. Zuverlässig funktionierende und sichere Software ist aber nicht nur ein Wettbewerbsvorteil für Unternehmen, sondern auch Voraussetzung für sichere Anwendungen etwa im Auto, der Medizin oder Sicherheitstechnik.

Das Bundesministerium für Bildung und Forschung fördert daher das Forschungsprojekt VERISOFT XT in den kommenden drei Jahren mit rund 12 Millionen Euro. Ziel ist die Erarbeitung eines Qualitätssiegels „Verified in Germany“. Dazu sollen Methoden und Werkzeuge für die formale Verifizierung des Designs von integrierten Computersystemen geschaffen werden. Das bedeutet, den mathematischen und maschinell überprüften Beweis zu erbringen, dass die betrachteten Computersysteme im Entwurf Null Fehler enthalten. Während im Vorläuferprojekt die mathematischen Grundlagen hierfür erarbeitet wurden, geht es bei VERISOFT XT um beispielhafte industrielle Anwendungen. Hierbei müssen Programme mit zehntausenden Zeilen Code verifiziert werden.

In dem Projektkonsortium arbeiten zehn Partner aus der Wirtschaft, - kleine und große Unternehmen -, sowie sieben Universitäten unter der Konsortialführung des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) zusammen. Das Vorhaben wird im Rahmen des BMBF-Programms IKT 2020 – Forschung für Innovationen durchgeführt.

Ein Anwendungsbeispiel kommt aus dem Automobilbereich. Ein Fahrzeug enthält heute durchschnittlich 50 Steuergeräte (ABS, EPS etc.) bestehend aus jeweils rund 300

Elektronikbauteilen. Beträgt die Ausfallrate jedes dieser 15.000 Bauteile aufgrund von Produktions-, Entwurfs- oder Betriebsfehlern eins zu einer Million, dann akkumuliert sich dieses scheinbar geringe Risiko zu einer Ausfallrate von 1,5 % für die gesamte Elektronik. Bei zu erwartender Verdopplung des Elektronikanteils in Fahrzeugen und Wegfall mechanischer Rückfallebenen verschärft sich dieses Problem entsprechend. In VERISOFT XT soll deshalb die Funktion und das Echtzeitverhalten eines kompletten Mikrokontrollersystems in einem Steuergerät, das eine sicherheitskritische Funktion im Fahrwerk eines Oberklassefahrzeuges implementiert, formal verifiziert werden.

Der Bedienkomfort und die Fülle von Funktionalität moderner Betriebssysteme führen gleichzeitig zu Sicherheitslücken und Angriffspunkten, die Hacker nutzen, um illegal an vertrauliche Daten zu kommen. Zwar existieren kleinere Betriebssysteme, die aufgrund ihrer Größe überschaubarer und damit vertrauenswürdiger bleiben. Diese bieten jedoch nicht den Komfort, den man beispielsweise von seiner Homebanking-Software erwarten würde. Der Hypervisor stellt eine Lösung für dieses Dilemma dar. Er ist, einfach ausgedrückt, ein Betriebssystem für Betriebssysteme und stellt sicher, dass es keinen unerlaubten Speicher-zugriff zwischen einzelnen Betriebssystemen gibt. Mit VERISOFT XT soll an einem konkreten Beispiel gezeigt werden, dass auch böswillige Anwender keine Chance haben, den verifizierten Hypervisor zu überlisten.

Weitere Anwendungsbeispiele und Informationen zu dem Projektverbund VERISOFT XT sind erhältlich bei http://www.verisoft.de