HomER rechnet auf Geheimnissen

Trau, schau, wem: Das Informatics Innovation Center (IIC) stellt am KIT sein Pilotprojekt HomER vor, das Rechnen auf verschlüsselten Daten ermöglicht.

HomER weist den Weg in die Zukunft der Datenverschlüsselung. Mit historischen Exponaten zeigt das IIC am 16. Februar auch ihre Vergangenheit (Foto: privat)

Monika Landgraf
Pressesprecherin (komm.)

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-47414
Fax: +49 721 608-43658

Weiterer Kontakt:

Prof. Dr. Jörn Müller-Quade
Institut für Kryptographie und Sicherheit (IKS)
Tel.: +49 721 608-44205
E-Mail: info@iks.kit.edu

Der Austausch sensibler Daten in Geschäftsvorgängen setzt gegenseitiges Vertrauen der Partner voraus. Sicherheit auch ganz ohne Vertrauen ist das Ziel von HomER (HOMomorphic Encryption Realization): Ein neuartiges hardwaregestütztes Verfahren erlaubt es zwei sich misstrauenden Teilnehmern, sichere Berechnungen auf geheimen Eingaben anzustellen. So könnten etwa Geschäftsdaten so abgeglichen werden, dass nur das gewünschte Ergebnis bekannt wird, die Eingaben aber geschützt bleiben.

Geschäftsprozesse wie beispielsweise Wertpapierhandel, Auktionen oder Ressourcenmanagement werden zunehmend verteilt durchgeführt. Für ihre Sicherheit wird bisher gegenseitiges Vertrauen vorausgesetzt. Mit sicheren Berechnungen, wie sie im Projekt HomER erforscht werden, wird die Sicherheit auch ohne dieses Vertrauen garantiert. So können beispielsweise Baufirmen bei öffentlichen Ausschreibungen, bei denen das Unternehmen mit dem niedrigsten Angebot den Zuschlag erhält, ihr Angebot geheim abgeben. Mittels

sicherer Berechnung kann dabei garantiert werden, dass die Konkurrenten keine Kenntnis von anderen Angeboten erlangen.

Zudem muss der Nutzer der im Projekt neu entwickelten Hardware weder dem Gerät vertrauen noch muss er dessen Aufbau kennen. Die Sicherheit des Verfahrens beruht auf der Isolation des Geräts von der Außenwelt, die über einen Faraday'schen Käfig sichergestellt wird.

HomER ist das Pilotprojekt des IIC, der Kooperation zwischen IBM Deutschland Research & Development, dem Karlsruher Institut für Technologie (KIT) und dem Forschungszentrum Informatik (FZI). Es untersucht insbesondere die neuen Möglichkeiten zur Umsetzung sicherer Berechnungen mit der bei IBM erfundenen vollhomomorphen Verschlüsselung (Fully Homomorphic Encryption), die ein Rechnen auf Geheimnissen erlaubt. Das IIC bietet Partnern aus der Industrie mehrere Mitgliedschaftsebenen an und ist aktiv an Public Private Partnerships interessiert.

Weitere Informationen unter http://www.iic.kit.edu

IBM Deutschland Research & Development GmbH, KIT und FZI präsentieren den Prototypen am **16. Februar 2011, 17:30 Uhr,** Institut für Kryptographie und Sicherheit (IKS) am KIT, Am Fasanengarten 5. Journalistinnen und Journalisten sind herzlich eingeladen.
Anmeldung bitte per E-Mail auf beiliegendem Formular.

Programm:

Begrüßung:
Professor Dr. Wilfried Juling, CSO/CIO des Karlsruher Instituts für Technologie (KIT)

Grußworte aus Politik und Wissenschaft

Grußworte:
Herr Sven Löschenkohl, Vice President - Leader Public Sector - IBM Deutschland GmbH

Keynote: "Cryptography: Magic, Science, or Science Fiction?"
Professor Dr. Dieter Gollmann, Institut für Sicherheit in verteilten Anwendungen, Technische Universität Hamburg-Harburg

Vorführung des Prototypen des HomER Projekts

Empfang (ca. 19:30 Uhr)

Medienvertreter haben während des Empfangs die Gelegenheit zu Interviews.

Ausstellung: Während des Empfangs wird eine kleine Auswahl historischer Verschlüsselungsmaschinen ausgestellt.

Das Karlsruher Institut für Technologie (KIT) ist eine Körperschaft des öffentlichen Rechts und staatliche Einrichtung des Landes Baden-Württemberg. Es nimmt sowohl die Mission einer Universität als auch die Mission eines nationalen Forschungszentrums in der Helmholtz-Gemeinschaft wahr. Das KIT verfolgt seine Aufgaben im Wissensdreieck Forschung – Lehre – Innovation.

Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu