PRESSEMITTEILUNG

Agentur für Innovation in der Cybersicherheit GmbH

Michael Lindner
Pressesprecher
Tel.: +49 (0) 151 4415 0645
E-Mail: presse@cyberagentur.de

Willy-Brandt-Straße 87
06110 Halle (Saale)

Halle (Saale), 23.11.2022

Mit neuen Verschlüsselungslösungen wird die Datensicherheit erhöht

Machbarkeitsstudie „Encrypted Computing“ an Cyberagentur übergeben

Forscherinnen und Forscher des CISPA Helmholtz-Zentrum für Informationssicherheit und des Instituts KASTEL am Karlsruher Instituts für Technologie (KIT) haben am Montag (21.11.2022) die Ergebnisse ihrer Machbarkeitsstudie zum Thema „Encrypted Computing“ an die Agentur für Innovation in der Cybersicherheit (Cyberagentur) übergeben.

Im Dezember 2021 hatte die Cyberagentur ihr erstes ausgeschriebenes Projekt zum Thema „Encrypted Computing“ an das CISPA Helmholtz-Zentrum für Informationssicherheit und an das Karlsruher Institut für Technologie (KIT), als Unterauftragnehmer, vergeben. Eine Machbarkeitsstudie sollte potenzielle „Encrypted Computing“-Anwendungen identifizieren, welche zukünftig im Bereich der Inneren und Äußeren Sicherheit eingesetzt werden können. Hierbei ging es zentral darum, die Sicherheitseigenschaften zu erfassen und einen Vergleich der Leistungsfähigkeit dieser Verfahren in Abhängigkeit von ihren Anwendungsszenarien zu erreichen.

Encrypted Computing und ähnliche Technologien gelten als zukunftsweisende Ansätze, um die Datensicherheit zu erhöhen. „Mit Kryptografie lassen sich Datenverarbeitung und Datenschutz vereinbaren“, sagt Prof. Dr. Jörn Müller-Quade vom Institut KASTEL am KIT. Bislang galt in der modernen Kryptographie, bevor man mit verschlüsselten Daten weiterarbeiten kann, muss man sie entschlüsseln. CISPA-Faculty Dr. Nico Döttling und Prof. Dr. Jörn Müller-Quade wollen daran etwas ändern. Beide Forscher sind Experten auf dem Gebiet des Encrypted Computing, einer Familie von Verschlüsselungsverfahren, mit denen Daten auch in verschlüsselter Form verarbeitet werden können. Eine Entschlüsselung zum Klartext ist erst dann wieder nötig, wenn die Ergebnisse eingesehen werden sollen, für Berechnungen ist dies aber nicht nötig. Sensible und sicherheitskritische Daten können so zwar analysiert, aber gleichzeitig auch geheim gehalten werden.

Insbesondere die Effizienz der derzeit bekannten Algorithmen für eine solche Kryptographie ist ein großes Problem für die Forschung. „Encrypted Computing ist keine Universallösung

Geschäftsführer:
Prof. Dr. Christian Hummert,
Daniel Mayer

Vorsitzender des Aufsichtsrats:
Dr. Christian Mrugalla

Mobil: +49 (0) 151 4415 0645
Telefon: +49 345 78288032
Telefax: +49 345 68558067

presse@cyberagentur.de
www.cyberagentur.de

für sicheres Rechnen. Allerdings birgt das Gebiet noch enormes Potenzial, insbesondere, wenn noch effizientere Algorithmen gefunden werden“, so Döttling. Müller-Quade ergänzt: „Insbesondere ist es derzeit keine Universallösung, weil es für manche Anwendungen vielleicht nicht effizient genug ist. Vielleicht gibt es für manche Anwendungen sogar prinzipielle Grenzen. Wir würden uns über ein Folgeprojekt freuen. Durch Technologieoffenheit können wir für verschiedene Sicherheitsniveaus effizientere Lösungen finden.“

„Unsere Mission ist es, innovative Technologien für Anwendungen in der inneren und äußeren Sicherheit zu fördern, die aber noch fernab von der Marktreife stehen“, sagt Robert Seidel, Projektverantwortlicher bei der Cyberagentur. „Encrypted Computing passt sehr gut in dieses Bild. Ich freue mich, dass wir in KASTEL/KIT und CISPA zwei so forschungsstarke Partner für unser Projekt gewinnen konnten.“ Die Machbarkeitsstudie ist der erste Schritt der Forschungsaktivitäten der Cyberagentur im Bereich des Encrypted Computing. Weitere Forschungsprogramme sollen folgen: „Bereits im kommenden Jahr wollen wir mit einer neuen Ausschreibung dafür werben, dass sich Kryptologinnen und Kryptologen weiterhin mit unseren Fragen auseinandersetzen“, sagt Projektmanagerin Dr. Tanja Zeeb.

Kontakt

Michael Lindner
Pressesprecher der Cyberagentur

Tel.: +49 151 44150 645
E-Mail: presse@cyberagentur.de
Internet: https://www.cyberagentur.de/

Über das CISPA:

Das CISPA Helmholtz-Zentrum für Informationssicherheit ist eine Großforschungseinrichtung des Bundes innerhalb der Helmholtz-Gemeinschaft. Die Wissenschaftlerinnen und Wissenschaftler erforschen die Informationssicherheit in all ihren Facetten. Sie betreiben modernste Grundlagenforschung sowie innovative anwendungsorientierte Forschung und arbeiten an drängenden Herausforderungen der Cybersicherheit, der Künstlichen Intelligenz und des Datenschutzes. CISPA-Forschungsergebnisse finden Einzug in industrielle Anwendungen und Produkte, die weltweit verfügbar sind. Damit stärkt das CISPA die Konkurrenzfähigkeit Deutschlands und Europas. Es fördert außerdem Talente und ist eine Kaderschmiede für hervorragend ausgebildete Fach- und Führungskräfte für die Wirtschaft. So trägt das CISPA sein Know-how auch in die Zukunft.

Über KASTEL:

KASTEL wurde als nationales Kompetenzzentrum für IT-Sicherheit vom Bundesministerium für Bildung und Forschung ins Leben gerufen. Seit dem 1. Januar 2021 ist es als dauerhafte Einrichtung am Karlsruher Institut für Technologie und in der Helmholtz-Gemeinschaft etabliert.

Als eine der international führenden Forschungseinrichtungen leistet KASTEL Beiträge zur interdisziplinären Erforschung ganzheitlicher Lösungen für Sicherheit und Datenschutz komplexer vernetzter Systeme. Dadurch wird der Bogen von der Grundlagenforschung zur Anwendungsforschung einschließlich des zeitnahen Transfers in Wirtschaft, Gesellschaft und Politik gespannt. KASTEL erforscht die Quantifizierung von Sicherheit und Privatsphäre und lässt sich dabei von der Einheit von Forschung, Lehre und Innovation leiten.

Über die Cyberagentur:

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) wurde im Jahr 2020 als vollständige Inhouse-Gesellschaft des Bundes unter der gemeinsamen Federführung des Bundesministeriums der Verteidigung und des Bundesministeriums des Innern und für Heimat durch die Bundesregierung mit dem Ziel gegründet, einen im Bereich der Cybersicherheit anwendungsstrategiebezogenen und ressortübergreifenden Blick auf die Innere und Äußere Sicherheit einzunehmen. Vor diesem Hintergrund bezweckt die Arbeit der Cyberagentur maßgeblich eine institutionalisierte Durchführung von hochinnovativen Vorhaben, die mit einem hohen Risiko bezüglich der Zielerreichung behaftet sind, gleichzeitig aber ein sehr hohes Disruptionspotenzial bei Erfolg innehaben können.

Der Cyberagentur stehen Prof. Dr. Christian Hummert als Forschungsdirektor und Geschäftsführer sowie Daniel Mayer als kaufmännischer Direktor vor.

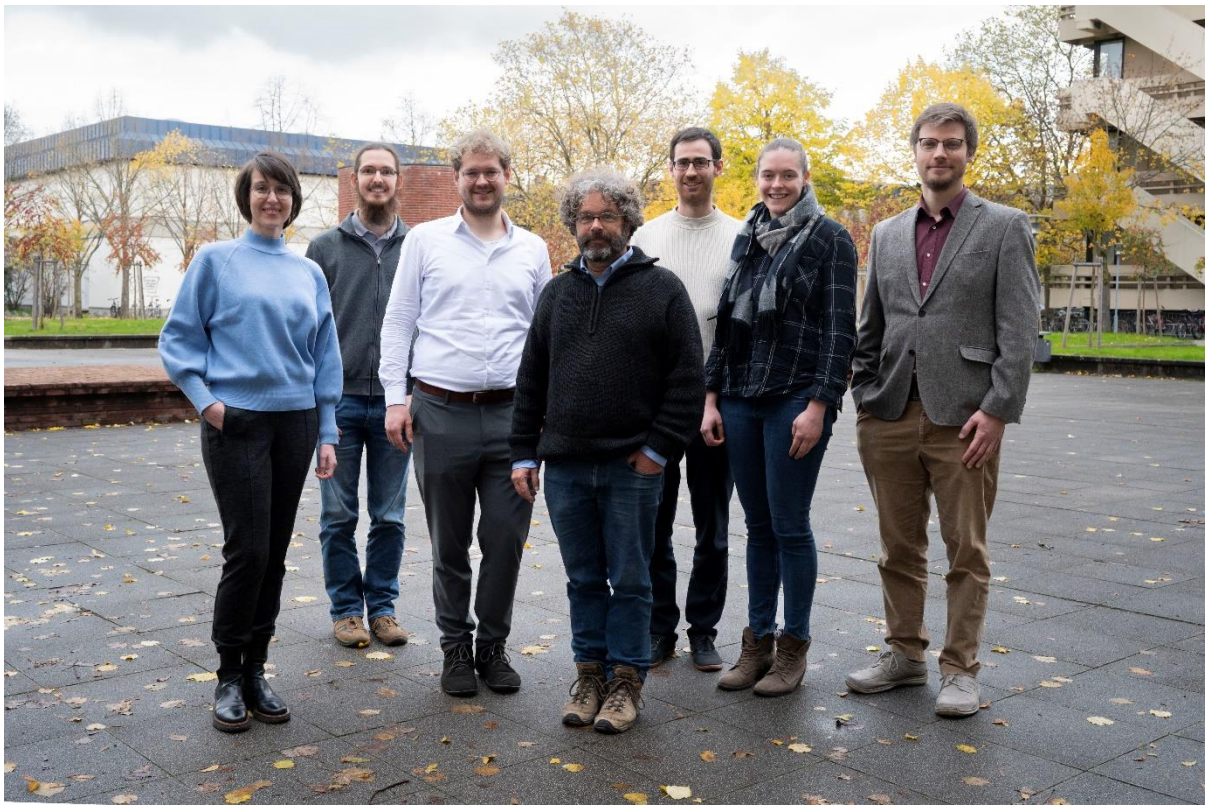
Im Dezember 2022 hatte die Cyberagentur ihr erstes ausgeschriebenes Projekt zum Thema „Encrypted Computing“ an das CISPA und das KIT vergeben. Eine Machbarkeitsstudie sollte potenzielle „Encrypted Computing“-Anwendungen identifizieren, welche zukünftig im Bereich der Inneren und Äußeren Sicherheit eingesetzt werden können. Hierbei ging es zentral darum, die Sicherheitseigenschaften zu erfassen und einen Vergleich der Leistungsfähigkeit dieser Verfahren in Abhängigkeit von ihren Anwendungsszenarien zu erreichen. [Link zur PM]

Geschäftsführer:
Prof. Dr. Christian Hummert,
Daniel Mayer

Vorsitzender des Aufsichtsrats:
Dr. Christian Mrugalla

Mobil: +49 (0) 151 4415 0645
Telefon: +49 345 78288032
Telefax: +49 345 68558067

presse@cyberagentur.de
www.cyberagentur.de



Das Projekt-Team (v.l.): Dr. Tanja Zeeb, Agentur für Innovation in der Cybersicherheit GmbH; Robin Berger, wiss. Mitarbeiter, Institut für Informationssicherheit und Verlässlichkeit am KIT; Dr. Robert Seidel, Agentur für Innovation in der Cybersicherheit GmbH; Prof. Dr. Jörn Müller-Quade, OE-Leitung, Institut für Informationssicherheit und Verlässlichkeit am KIT; Laurin Benz, wiss. Mitarbeiter, Institut für Informationssicherheit und Verlässlichkeit am KIT; Anne Müller, CISPA Helmholtz Center for Information Security; Dr. Nico Döttling, CISPA Helmholtz Center for Information Security Foto: KASTEL

Geschäftsführer:
Prof. Dr. Christian Hummert,
Daniel Mayer

Vorsitzender des Aufsichtsrats:
Dr. Christian Mrugalla

Mobil: +49 (0) 151 4415 0645
Telefon: +49 345 78288032
Telefax: +49 345 68558067

presse@cyberagentur.de
www.cyberagentur.de