idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Technische Universität Darmstadt
Silke Paradowski

29.10.2018
http://idw-online.de/de/news704958

Forschungs- / Wissenstransfer, Forschungsergebnisse
Informationstechnik
überregional

Forscher präsentieren Krypto-Assistenten für Software-Entwickler

Darmstadt, 29. Oktober 2018. Wissenschaftler der TU Darmstadt haben in Zusammenarbeit mit der Universität Paderborn und dem Fraunhofer-Institut für Entwurfstechnik Mechatronik einen „Kryptographie-Assistenten" für besseren Datenschutz vorgestellt. CogniCrypt unterstützt Software-Entwickler bei der Integration von Kryptographie-Komponenten in ihre Software und überprüft den korrekten Einbau und die Konfiguration.

Nicht erst seit den großen Datenschutz-Skandalen ist die Sicherheit von Software für deren Nutzer ein wichtiges Auswahlkriterium. Deswegen achten viele darauf, dass die von ihnen benutzten Anwendungen zum Beispiel Verschlüsselung anbieten. Doch selbst das ist keine Garantie für Datensicherheit: Software-Entwickler haben meistens keine Erfahrung mit Kryptographie – und bauen deswegen die Krypto-Bausteine fehlerhaft ein. Das Ergebnis: Die Anwendungen sind trotz vermeintlich eingebauter Verschlüsselung unsicher.

Um dem abzuhelfen, haben Wissenschaftler der TU Darmstadt im Rahmen des von der Deutschen Forschungsgemeinschaft geförderten Sonderforschungsbereichs CROSSING nun CogniCrypt, einen „Kryptographie-Assistenten" für Software-Entwickler, vorgestellt. Diese können ab sofort weltweit auf dieses Werkzeug zugreifen. Um die Benutzung so einfach wie möglich zu machen, wurde CogniCrypt so eingerichtet, dass es sich nahtlos in den Workflow der Entwickler einbinden lässt. Der Krypto-Assistent lässt sich auf der weitverbreiteten „Eclipse"-Plattform für integrierte Entwicklungssoftware-Werkzeuge installieren, die von vielen Programmiererinnen und Programmierern verwendet wird, und ist auch direkt über den Eclipse-Marketplace verfügbar.

„CogniCrypt erlaubt es Entwicklern, nicht nur Krypto-Fehlbenutzungen in ihrem Programmcode zu erkennen, sondern gibt auch Ratschläge für die Behebung dieser Schwachstelle", erläutert Informatik-Professorin Mira Mezini von der Technischen Universität Darmstadt. „Das Tool erlaubt es ihnen sogar, automatisch Programmcode für die sichere Integration von Kryptographie zu generieren. Das ist auch bitter nötig: In einer großangelegten Studie mit CogniCrypt fanden wir heraus, dass gut drei Viertel aller Anwendungen Kryptographie auf unsichere Weise einbetten."

„Für CogniCrypt haben wir eine eigene Beschreibungssprache – Crypto Specification Language (CrySL) – entwickelt, mit der Kryptographen die Benutzungsregeln ihrer entwickelten Krypto-Komponenten definieren können, so dass CogniCrypt den Anwendungsentwicklern Hinweise über die richtige Benutzung der Krypto-Komponenten textbasiert und ohne Auseinandersetzung mit dem Quellcode präsentieren kann. In Zukunft planen wir sogar die automatisierte Generierung dieser Texthinweise. Das macht es für Kryptographen einfacher, ihre Krypto-Komponenten in CogniCrypt zu integrieren", erklärt Professor Eric Bodden vom Heinz Nixdorf Institut der Universität Paderborn und vom Fraunhofer-Institut für Entwurfstechnik Mechatronik (IEM) und einer der beteiligten Wissenschaftler im Sonderforschungsbereich CROSSING der TU Darmstadt.

Als Open Source verfügbar

CogniCrypt ist als Eclipse Open Source Projekt verfügbar. So können Kryptographen anderer Universitäten und Forschungseinrichtungen überprüfen, ob CogniCrypt die erforderlichen Prüfungen des Anwendungscodes auch korrekt umsetzt. Auch neue Krypto-Bausteine können hinzugefügt werden. Zusammen mit dem Feedback der Software-Entwickler, die ebenfalls neue Funktionen vorschlagen und hinzufügen können, soll eine lebendige Community um CogniCrypt herum entstehen. So bleibt der Krypto-Assistent durch die Kraft der Gemeinschaft immer aktuell und verbessert sich ständig weiter.

Entwickelt wurde CogniCrypt im Sonderforschungsbereich CROSSING an der TU Darmstadt in Zusammenarbeit mit der Universität Paderborn und dem Fraunhofer IEM. Mehr als 65 Wissenschaftlerinnen und Wissenschaftler aus Kryptographie, Quantenphysik, Systemsicherheit und Softwaretechnik arbeiten in CROSSING zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Ziel ist es, Sicherheitslösungen zu entwickeln, die auch in der Zukunft sichere und vertrauenswürdige IT-Systeme ermöglichen. CROSSING wird seit 2014 und bis 2022 von der Deutschen Forschungsgemeinschaft gefördert.

Weitere Infos: www.cognicrypt.de
Twitter: @cognicrypt
www.crossing.tu-darmstadt.de

Über die TU Darmstadt
Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 312 Professorinnen und Professoren, 4.450 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie knapp 26.000 Studierenden. Mit der Goethe-Universität Frankfurt und der Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

www.tu-darmstadt.de