Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Mehr Sicherheit für Alexa, Siri & Co.

Team der TU Darmstadt entwickelt Prototyp für Privatsphäre-schützende Spracherkennung

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Silke Paradowski
Tel. 06151 16 - 20019
Fax 06151 16 - 23750
paradowski.si@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de

Darmstadt, 31. August 2018. Im Profilbereich Cybersecurity der TU Darmstadt arbeiten Wissenschaftlerinnen und Wissenschaftler an verschiedensten Herausforderungen im Bereich von IT-Sicherheit und Privatheit. Das Thema sichere sprachgesteuerte Dienste ist ein Beispiel für Spitzenforschung, wie sie künftig im neuen Gebäude am Kantplatz stattfinden wird, für das heute Richtfest gefeiert wurde.

Mittlerweile sind sie im Leben vieler Nutzerinnen und Nutzer allgegenwärtig: Amazons „Alexa“, Apples „Siri“, Googles Assistant oder Microsofts „Cortana“ stehen mehr als zwei Milliarden Smartphone-Nutzern jederzeit zur Verfügung. Gleichzeitig steigt die Zahl von Smart-Home-Geräten wie Amazon Echo, Apple HomePod, oder Google Home. Und auch im Unternehmensumfeld werden digitale Assistenten zur Steigerung der Produktivität erprobt.
Zwecks Spracherkennung werden dafür jedoch kontinuierlich Audioaufzeichnungen in die Cloud übertragen. Das birgt erhebliche Risiken, denn diese Aufnahmen enthalten sensible biometrische Daten und potentiell vertrauliche Informationen. Gerieten diese in die falschen Hände, drohte neben dem Verlust von (Betriebs-)Geheimnissen zusätzliche Gefahr, zum Beispiel durch „Fake Recordings“. Das sind authentisch wirkende, jedoch künstlich erzeugte Sprachaufnahmen mit kompromittierendem Inhalt.
Um solche Bedrohungen bestmöglich einzudämmen, haben Wissenschaftler der TU Darmstadt unter der Leitung von Professor Ahmad-Reza Sadeghi und Professor Thomas Schneider gemeinsam mit dem Spracherkennungsexperten Professor Korbinian Riedhammer von der Hochschule Rosenheim eine neue Softwarearchitektur namens „VoiceGuard“ entwickelt. VoiceGuard nutzt Intel Software Guard Extensions (SGX), um die Sprachverarbeitungsprozesse von den Systemen des Dienstanbieters oder alternativ des Nutzers vollständig zu isolieren und sämtliche Daten zu schützen. Hierdurch wird sowohl die Privatsphäre des Nutzers als auch das geistige Eigentum des Dienstanbieters geschützt.

Die Evaluierung eines ersten Prototypen zeigt, dass VoiceGuard Privatsphäre-schützende Spracherkennung sogar in Echtzeit ermöglicht. Dank der generischen Architektur kann das Konzept auch für vergleichbare Aufgaben wie das Erkennen von Emotionen erweitert werden. VoiceGuard wird im September auf der INTERSPEECH 2018 vorgestellt, der internationalen Top-Konferenz im Bereich Sprachverarbeitung.

Kontakt

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
E-Mail: ahmad.sadeghi@trust.tu-darmstadt.de
Tel.: 06151/16-25328
https://www.trust.tu-darmstadt.de

Prof. Dr.-Ing. Thomas Schneider
E-Mail: schneider@encrypto.cs.tu-darmstadt.de
Tel.: 06151/16-27300
https://www.encrypto.cs.tu-darmstadt.de

Die Veröffentlichung zu „VoiceGuard“

VoiceGuard: Secure and Private Speech Processing.
https://encrypto.de/papers/BFRSSW18.pdf
Ferdinand Brasser, Tommaso Frassetto, Korbinian Riedhammer, Ahmad-Reza Sadeghi, Thomas Schneider, Christian Weinert

Mehr zum Thema Cybersicherheit aus dem Profilbereich CYSEC

Schwachstellen in Java-Script-basierten Webseiten aufgedeckt:
https://bit.ly/2wDPt47

Ein Rezept gegen die Macht der Quantencomputer:
https://bit.ly/2NttHqS

Mit Honeypots gut organisiert gegen Hacker-Netzwerke:
https://bit.ly/2MWdGwA

Der Profilbereich: www.cysec.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

MI-Nr. 44/2018, Weinert/Braun