Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Preisgekrönter Schutz für die Privatsphäre

Zweiter Platz für Forscher der TU Darmstadt beim 8. Deutschen IT-Sicherheitspreis

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

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

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

Darmstadt, 12. Februar 2021. Ein Forschungs-Team der Technischen Universität Darmstadt und der Technischen Universität Graz ist für die gemeinsame Einreichung „ContactGuard“ mit dem zweiten Platz des renommierten Deutschen IT-Sicherheitspreis der Horst Görtz-Stiftung ausgezeichnet worden. Das ContactGuard-Verfahren macht die Kontaktermittlung in mobilen Messenger-Apps sicherer.

Die Sicherheitsforscher Professor Thomas Schneider und Christian Weinert, Fachgebiet ENCRYPTO am Fachbereich Informatik der TU Darmstadt, wurden mit dem zweiten Platz des Deutschen IT-Sicherheitspreis der Horst Görtz-Stiftung geehrt. Zusammen mit TU-Darmstadt-Absolvent Matthias Senker sowie Professor Christian Rechberger und Daniel Kales (beide TU Graz) erhielten sie den zweiten Preis für „ContactGuard“, die Entwicklung eines Privatsphäre-schützenden Verfahrens zur Kontaktermittlung in Messenger-Diensten. Die achte Verleihung des höchstdotierten Preises für IT-Sicherheit in Deutschland fand am 11. Februar digital im Rahmen der ersten Innovationskonferenz Cybersicherheit statt. Eine Expertenjury wählte aus 46 Einreichungen die besten markt-relevanten Innovationen in der IT-Sicherheit. Mit dem zweiten Platz ist ein Preisgeld von 60.000 Euro verbunden.

In der ausgezeichneten Forschungsarbeit beschäftigte sich das Team mit Privatsphäre-schützenden Methoden zur Ermittlung von Kontakten in Messenger-Anwendungen wie WhatsApp, Signal und Telegram. Diese Dienste erlauben Nutzenden, bequem mit allen Personen in ihrem Adressbuch in Kontakt zu treten, die ebenfalls den Dienst verwenden. Derzeit eingesetzte Verfahren übermitteln dazu meist alle Adressbuch-Kontakte an den Dienstanbieter oder verwenden unsichere Schutzmechanismen – ein schwerwiegender Eingriff in die Privatsphäre, der auch datenschutzrechtliche Herausforderungen im Unternehmenseinsatz zur Folge hat. Mit „ContactGuard“ können Adressbucheinträge auf mobilen Geräten in zwei Schritten effektiv geschützt und Kontakte zwischen Nutzenden und Dienstleistern sicher ausgetauschten werden: Eine Erweiterung der Adressbuch-Anwendung ermöglicht, besonders schützenswerte Kontakte als „sensitiv“ zu kennzeichnen. Auf diese Kontakte erhalten Messenger keinen Zugriff. Für die verbleibenden Kontakte werden als sicher bewiesene und sehr effiziente kryptographische Protokolle zur privaten Schnittmengenberechnung innerhalb der Messenger-Anwendung ausgeführt. Dabei werden die Adressbücher so verarbeitet, dass der

Dienstanbieter keinerlei Informationen über Kontakte erhält, die nicht registriert sind.
Kontaktermittlungsverfahren von mobilen Messenger-Diensten Privatsphäre-schützend zu gestalten ist ein bislang ungelöstes Problem mit hoher praktischer Relevanz. An entsprechenden Lösungsansätzen forscht das von Professor Thomas Schneider geleitete Fachgebiet ENCRYPTO in Zusammenarbeit mit der Bar-Ilan University (Israel) und der Aalto University (Finnland) bereits seit 2014. Praktikabel wurde die Privatsphäre-schützende Kontaktermittlung mit „ContactGuard“ jedoch erst durch eine neue Generation kryptographischer Protokolle. Die Dringlichkeit solcher Lösungen wird durch eine jüngst vom Fachgebiet ENCRYPTO zusammen mit der Universität Würzburg durchgeführte Studie verdeutlicht, die zeigt, dass bisher eingesetzte Schutzverfahren zur Kontaktermittlung in Messenger-Apps in nur wenigen Millisekunden gebrochen werden können.

Erfolg für Sonderforschungsbereich CROSSING

Professor Thomas Schneider ist Principal Investigator im Kryptographie-Sonderforschungsbereich CROSSING an der TU Darmstadt. CROSSING stellt alle drei Preisträgerinnen und Preisträger des diesjährigen Deutschen IT-Sicherheitspreises:
Die Trägerin des ersten Preises, Dr. Haya Shulman (Fraunhofer SIT), ist ebenfalls Mitglied bei CROSSING und gewann den Sicherheitspreis mit ihrer Arbeit „CacheTest“. Das Projekt beschäftigt sich mit Sicherheitslücken, die bei der Übersetzung von www-Adressen in Internetadressen entstehen. Die Entwicklung erkennt die Fälschung von Webseitenadressen, und verhindert so beispielsweise die Weiterleitung zu gefälschten Onlinebanking-Webseiten.
Der dritte Platz des IT-Sicherheitspreises ging an Tobias Cloosters, Michael Rodler und Professor Lucas Davi (alle Universität Duisburg-Essen) für ihre Entwicklung „TeeRex“, ein automatisiertes Analysetool zur Suche von Schwachstellen in sogenannten Trust Execution Environments (TEEs), besonders abgesicherten Einheiten in den Hauptprozessoren von Rechnern und Smartphones. Davi promovierte an der TU Darmstadt, war Claude-Shannon-Fellow am damaligen Profilbereich Cybersicherheit der TU und ist Principal Investigator im Sonderforschungsbereich CROSSING.

Schließlich schaffte es das Projekt „Perun“ unter die elf Finalisten des IT-Sicherheitspreises. Daran beteiligt ist am Fachbereich Informatik der TU Darmstadt das Fachgebiet Angewandte Kryptografie mit Professor Sebastian Faust und Hendrik Amler, zusammen mit Dr. Lisa Eckey, Sasan Safai und Sebastian Stammler (Perun) sowie Kristina Hostáková (ETH Zürich) und Professor Stefan Dziembowski (Uni Warschau). Die Off-Chain-Technologie „Perun“ macht Blockchains vielfältiger einsetzbar und sicherer.

Der Deutsche IT-Sicherheitspreis zählt mit insgesamt 200.000 Euro zu den höchst dotierten privat gestifteten Wirtschaftspreisen in Deutschland. Bewertet werden innovative Ideen für Sicherheit und Privatsphärenschutz, die in der Praxis über reale Marktchancen verfügen. Im Sinne des Preisstifters und Ehrensenators der TU Darmstadt, Dr.-Ing. E.h. Horst Görtz, sollen die Preisgelder für die Weiterentwicklung der prämierten Konzepte oder Lösungen zur Erlangung der Marktreife eingesetzt werden.

Veröffentlichung zu ContactGuard

Mobile Private Contact Discovery at Scale von Daniel Kales (TU Graz), Christian Rechberger (TU Graz), Thomas Schneider (TU Darmstadt), Matthias Senker (TU Darmstadt) und Christian Weinert (TU Darmstadt), in: 28. USENIX Security Symposium (USENIX Security'19). Online: https://ia.cr/2019/517.

Weiterführende Veröffentlichungen

Private Set Intersection for Unequal Set Sizes with Mobile Applications von Ágnes Kiss (TU Darmstadt), Jian Liu (Aalto University), Thomas Schneider (TU Darmstadt), N. Asokan (Aalto University) und Benny Pinkas (Bar-Ilan University), in: Proceedings on Privacy Enhancing Technologies (PoPETs'17). Online: https://ia.cr/2017/670.

All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers von Christoph Hagen (Universität Würzburg), Christian Weinert (TU Darmstadt), Christoph Sendner (Universität Würzburg), Alexandra Dmitrienko (Universität Würzburg) und Thomas Schneider (TU Darmstadt), in: 28. Annual Network and Distributed System Security Symposium (NDSS'21). Online: https://ia.cr/2020/1119.

Links

Erklär-Video „Kontakte teilen & trotzdem Privatsphäre schützen mit Private Set Intersection“: https://youtu.be/P_K166jvG7U

Webseite des Fachgebiets ENCRYPTO: https://encrypto.de

Kontakt:

Prof. Dr.-Ing. Thomas Schneider
Tel.: 06151/16-27300
E-Mail: schneider@encrypto.cs.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. Drei Forschungsfelder prägen das Profil der TU Darmstadt: I+I (Information and Intelligence), E+E (Energy and Environment) sowie M+M (Matter and Materials). 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, rund 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie rund 25.400 Studierenden. Im Netzwerk UNITE!, das Universitäten aus sieben europäischen Ländern vereint, treibt die TU Darmstadt die Idee der europäischen Universität voran. 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. 09/2021, Fleckenstein/Braun/sip