idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Technische Universität München
Julia Rinner

05/15/2025
http://idw-online.de/en/news852255

Research results, Scientific Publications
Information technology
transregional, national

Sechsecke für den Datenschutz: Nachweis des Standorts ohne persönliche Daten preiszugeben

Standortdaten gelten als besonders sensibel – ihr Missbrauch kann schwerwiegende Folgen haben. Forschende der Technischen Universität München (TUM) haben ein Verfahren entwickelt, das es erlaubt, den eigenen Standort kryptografisch zu beweisen – ohne diesen preiszugeben. Die Grundlage hierfür bildet der sogenannte Zero-Knowledge-Beweis mit standardisierten Gleitkommazahlen.

Zahlreiche Apps auf dem Handy zeichnen ununterbrochen den Standort auf – oftmals ohne dass es Nutzerinnen und Nutzer bemerken. Anhand von Bewegungsprofilen können Anbieter daraus Schlüsse über den Arbeitsort, Gewohnheiten und persönliche Vorlieben ziehen. Welche Folgen das Sammeln solcher sensiblen Informationen haben kann, zeigt eine investigative Recherche der New York Times aus dem Jahr 2019. Auf Grundlage kommerzieller Standortdaten konnte innerhalb weniger Minuten ein Endgerät eines Mitglieds von Präsident Trumps Entourage zugeordnet werden – inklusive Aufenthalten an sensiblen Orten wie Mar-a-Lago oder dem Pentagon.

Der Standort als Beweis – ohne Preisgabe der Koordinaten

Um zukünftig ein Verfahren zur Verfügung zu stellen, das die Privatsphäre schützt und gleichzeitig nachweisbare Standortdaten liefert, greifen Forschende auf sogenannte Zero-Knowledge-Beweise zurück. Dabei handelt es sich um mathematische Beweise, mit denen sich die Gültigkeit einer Aussage nachweisen lässt, ohne dabei die zugrundeliegenden Daten offenzulegen. Der Clou: Die Methode erlaubt eine frei wählbare Genauigkeit der Angaben, abgestimmt auf den jeweiligen Anwendungsfall.

„Die Herausforderung besteht darin, Datenschutz und Genauigkeit miteinander zu vereinen – und zwar so, dass das Verfahren auch praktisch einsetzbar ist“, erklärt Jens Ernstberger, der Erstautor der Studie. Das ist dem Forschungsteam an der Professur für Embedded Systems and Internet of Things gelungen, indem sie Zero-Knowledge-Beweise mit einem präzisen Geogitter kombinieren. Um den eigenen Standort verifizierbar, aber nicht offen darzustellen, nutzt die Methode ein hierarchisches Sechseck-Gittersystem. Dieses Gitter teilt die Erdoberfläche in Zellen auf, die sich in unterschiedlichen Auflösungen darstellen lassen – von der groben Regionalebene bis hinunter zu einzelnen Straßenabschnitten. Nutzerinnen oder Nutzer können so beispielsweise entscheiden, ob sie preisgeben, dass sie sich in einer bestimmten Stadt befinden oder, falls höhere Genauigkeit gewünscht ist, in einem bestimmten Park dieser Stadt. In beiden Fällen bleibt ihre genaue Position verborgen.

Gleitkommazahlen verbessern die Positionsbestimmung

Die eigentliche Innovation der aktuellen Studie steckt in der mathematischen Verarbeitung der Standortdaten in den Zero-Knowledge-Beweisen: Anders als bisherige Systeme, die oft auf fehleranfälliger Ganzzahlarithmetik basieren, verwendet das neue Verfahren standardisierte Gleitkommazahlen, wie sie auch von modernen Computern verarbeitet werden. Dieser Schritt ist entscheidend, um Rechengenauigkeit zu garantieren und ungewollte Abweichungen zu

vermeiden, insbesondere bei komplexen Operationen wie Wurzeln oder trigonometrischen Funktionen. Zugleich umgeht der neue Ansatz Fehler, die bei bisherigen Implementierungen zu falschen Ergebnissen oder Sicherheitslücken führen konnten. Der Zero-Knowledge-Beweis lässt sich dabei innerhalb weniger Millisekunden berechnen.

Einsatz im Alltag denkbar

Ein Beispiel für die Anwendung ist das Peer-to-Peer Proximity Testing. Damit lässt sich feststellen, ob sich zwei Personen in räumlicher Nähe befinden – ohne dass eine von beiden ihre genaue Position offenlegen muss. In einem Prototyp kann ein Nutzer in nur 0,26 Sekunden beweisen, dass er sich in der Nähe einer bestimmten Region befindet. Gleichzeitig lässt sich die gewünschte Genauigkeit flexibel anpassen: Statt den exakten Standort zu belegen, kann die Person beweisen, dass sie sich in einem bestimmten Stadtviertel oder Park befindet.

„Unsere Methode zeigt, dass Standortnachweise unter Wahrung der Privatsphäre möglich und performant sind“, sagt Prof. Sebastian Steinhorst, Professor für Embedded Systems and Internet of Things.

Darüber hinaus bietet die Arbeit auch einen allgemeinen Beitrag zur Kryptografie: Die entwickelten Gleitkommazahl-Schaltungen der Zero-Knowledge-Beweise sind unabhängig vom konkreten Anwendungsfall wiederverwendbar und könnten künftig auch in anderen Bereichen zum Einsatz kommen – etwa bei der Verifikation physikalischer Messdaten oder im Bereich sicherer maschineller Lernsysteme. Das eröffnet neue Perspektiven für vertrauenswürdige Systeme, etwa in der digitalen Gesundheitsvorsorge, in Mobilitätsanwendungen oder im Identitätsschutz.

contact for scientific information:

Prof. Dr. Sebastian Steinhorst
Technische Universität München
Professur für Embedded Systems and Internet of Things
sebastian.steinhorst@tum.de
www.tum.de

Original publication:

Ernstberger, J., Zhang, C., Ciprian, L., Javanovic, P., Steinhorst, S. Zero-Knowledge Location Privacy via Accurate Floating-Point SNARKs. IEEE Symposium on Security and Privacy (2025). DOI: 10.1109/SP61157.2025.00057

URL for press release:
https://www.tum.de/aktuelles/alle-meldungen/pressemitteilungen/details/sechsecke-fuer-den-datenschutz