Privacy: Schweigepflicht für das digitale Sparschwein

Bonuspunktekarten und digitales Bezahlen sind populär, aber ihre Nutzer hinterlassen eine Datenspur – Wissenschaftler vom KIT entwickeln System zum besseren Schutz der Privatsphäre

Mit ihrer Bonuskarte sammeln Konsumenten beim Bezahlen Punkte. Kryptographische Methoden könnten dabei die Privatsphäre besser schützen. (Bild: KIT)

„Sammeln Sie Bonus-Punkte“? Diese Frage gehört mittlerweile zum Einkaufsalltag. Mehr als 80 Prozent der deutschen Haushalte beteiligen sich an Bonusprogrammen. Sie laufen Gefahr, sensible Informationen über sich preiszugeben, wenn ein solches System missbraucht wird. Die Arbeitsgruppe Kryptographie und Sicherheit am Karlsruher Institut für Technologie (KIT) entwickelt deswegen ein digitales Bonus- und Bezahlsystem, das einerseits die Anonymität der Kunden sicherstellt, andererseits den Betreibern die gewünschten Mehrwerte bieten soll.

„Nur die wenigsten Verbraucher machen sich Gedanken darüber, was man aus ihren Daten alles ablesen kann“, erklärt Andy Rupp, Experte für Kryptographie am KIT. In heutigen Systemen kann jeder Einkauf und jedes Produkt mit den persönlichen Angaben verknüpft werden, welche die Kunden bei der Registrierung hinterlassen. Selbst ohne die explizite Angabe von Kundendaten, besteht ein hohes Risiko der Verknüpfung von Einkäufen und Kundenidentität. Damit entstehen Bewegungs- und Personenprofile, die Rückschlüsse zulassen

KIT-Zentrum Information • Systeme • Technologien

Monika Landgraf
Pressesprecherin

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-47414
Fax: +49 721 608-43658
E-Mail: presse@kit.edu

Weiterer Kontakt:

Kosta Schinarakis
Themenscout
Tel.: +49 721 608 41956
Fax: +49 721 608 43658
E-Mail: schinarakis@kit.edu

nicht nur auf das Kaufverhalten der Menschen, sondern etwa auch auf ihren Gesundheitszustand oder ihre persönlichen Vorlieben.

In heutigen Systemen führt das Endgerät des Kunden - eine Smartcard oder ein Smartphone - zum Punktesammeln praktisch keine Berechnungen aus. Es sendet nur eine Identifikationsnummer, mit der sich die neuen Bonuspunkte im Back-End des Betreibers einem Kundenkonto zuordnen lassen. Rupp und sein Forschungskollege Tibor Jager von der Universität Paderborn wollen diese Endgeräte intelligenter machen: Die Geräte speichern selbst den Punktestand und führen gemeinsam mit dem Betreiber kryptographische Algorithmen aus. Diese erlauben es, Punkte sicher und unter dem Schutz der Privatsphäre zu addieren oder zu subtrahieren. „Das Ganze funktioniert wie ein digitales Sparschwein, dessen Sicherheitseigenschaften mathematisch nachweisbar sind“, sagt Rupp. Niemand außer dem Kunden erfährt woher die Bonuspunkte stammen und wie viele er in den einzelnen Geschäften sammelt.

Das Einkaufen wird dank digitaler Systeme einfacher, aber hinterlässt auch umfangreiche Datenspuren. (Bild: KIT)

„Mit unserer Forschung wollen wir die Bürger für die Bedeutung von Privacy in der digitalen Welt sensibilisieren“, betonen Rupp und sein Team. Das digitale Sparschwein könnte unter anderem auch bei sogenannten Stored-Value-Cards – Geldkarten, die zum Beispiel der ÖPNV einsetzt – zur Anwendung kommen. Ein weiteres, in naher Zukunft relevantes Szenario ist das Vehicle-to-Grid-System (V2G). Bei V2G speisen Elektroautos in Zeiten, in denen zu wenig Energie zur Verfügung steht, Strom ins öffentliche Netz ein. Hierfür registrieren Server auf Parkplätzen die Zahl der Elektroautos und ihre jeweilige Kapazität und koordinieren die Einspeisung mit dem aktuellen Bedarf. Die Besitzer der Fahrzeuge erhalten dafür eine monetäre Entschädigung. In beiden Anwendungsfällen soll das neue System die Berechnung von Bewegungsprofilen verhindern.

Ein Prototyp läuft mit Kernfunktionalitäten bereits auf dem Smartphone. Das Forschungsteam will ihn jetzt zum einen für den Einsatz auf Smartcards optimieren und zum anderen seine Funktionalität für unterschiedliche Applikationen weiter ausbauen. Ein wichtiges Feature wäre zum Beispiel Bonuskartensysteme zu ermöglichen, die die Privatsphäre wahren. Betreiber könnten dann gezielt Statistiken berechnen, ohne kundenbezogene Daten zu erhalten.

Mehr zur Forschung:

crypto.iti.kit.edu/index.php?id=cyphycrypt

degruyter.com/view/j/popets.2016.2016.issue-3/popets-2016-0016/popets-2016-0016.xml

Details zum KIT-Zentrum Information · Systeme · Technologien (in englischer Sprache): http://www.kcist.kit.edu

Das Karlsruher Institut für Technologie (KIT) verbindet seine drei Kernaufgaben Forschung, Lehre und Innovation zu einer Mission. Mit rund 9 300 Mitarbeiterinnen und Mitarbeitern sowie 25 000 Studierenden ist das KIT eine der großen natur- und ingenieurwissenschaftlichen Forschungs- und Lehreinrichtungen Europas.

KIT – Die Forschungsuniversität in der Helmholtz-Gemeinschaft

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu

Die Fotos stehen auf www.kit.edu zum Download bereit und können angefordert werden unter: presse@kit.edu oder +49 721 608-47414. Die Verwendung der Bilder ist ausschließlich in dem oben genannten Zusammenhang gestattet.