

Sicheres Bezahlen ohne Datenspur

17.10.2017, 12:00 | Wissenschaft, Forschung, Bildung

Pressemitteilung von: *Karlsruher Institut für Technologie*

Presseagentur: *Karlsruher Institut für Technologie*



Bezahlen mit dem Smartphone wird im Nahverkehr immer beliebter. Aber ist es auch sicher? (Foto: Gabi Zachmann/KIT)

Ob als Smartphone-App für die Fahrkarte im Nahverkehr, als Geldwertkarten für das Schwimmbad oder in Form einer Bonuskarte für den Supermarkt: Für viele gehören „elektronische Geldbörsen“ längst zum Alltag. Doch vielen Kunden ist nicht klar, dass sie mit der Nutzung dieser Angebote weitestgehend auf ihre Privatsphäre verzichten. Am Karlsruher Institut für Technologie (KIT) entsteht ein sicheres und anonymes System, das gleichzeitig Alltagstauglichkeit verspricht. Es wird nun auf der Konferenz ACM CCS 2017 in den USA vorgestellt.

Es ist vor allem das fehlende Problembewusstsein, das den Informatiker Andy Rupp von der Arbeitsgruppe „Kryptographie und Sicherheit“ am KIT immer wieder erstaunt: „Den wenigsten Nutzern ist nach meiner Beobachtung klar, dass sie mit der Teilnahme an solchen Bonus- oder Zahlungssystemen detailgetreu offenlegen wie und was sie konsumieren oder welche Wege sie zurücklegen.“ Denn um eine Manipulation der Konten durch unehrliche Nutzer vorzubeugen, werden die Kundendaten und Kontostände bei Zahlungs- und Bonussystemen heute standardmäßig mit Hilfe einer zentralen Datenbank verwaltet. Der Kunde wird bei jedem Zahlungsvorgang identifiziert und die Details seiner Transaktion der zentralen Datenbank mitgeteilt. Dieser wiederholte Identifikationsvorgang führt zu einer Datenspur, die durch den Anbieter oder durch Dritte missbraucht werden könnte.

Mit dem scheinbaren Widerspruch von Privatsphäre und Sicherheit wollte sich der Kryptographie-Experte nicht abfinden und hat nun gemeinsam mit Gunnar Hartung und Matthias Nagel vom KIT sowie Max Hoffmann von der Ruhr-Universität Bochum die Grundlagen einer „elektronischen Geldbörse“ vorgestellt, die anonym funktioniert, gleichzeitig aber Missbrauch verhindert. Das von ihnen entwickelte Protokoll „black-box accumulation plus“ (BBA+) verlagert dabei alle notwendigen Kontoinformationen auf die verwendete Karte oder das Smartphone und garantiert mithilfe kryptographischer Methoden deren Vertraulichkeit. Gleichzeitig bietet BBA+ aber auch Sicherheitsgarantien für den Betreiber des Bonus- oder Zahlungssystems: Das Protokoll garantiert den korrekten Kontostand und ist mathematisch zudem so konstruiert, dass die Identität eines Nutzers aufgedeckt wird, sobald versucht wird, mit einem manipulierten Konto zu bezahlen.

Das neue Protokoll ist die Weiterentwicklung eines anonymen Bonuskartensystems, das ebenfalls von der KIT-Forschungsgruppe entwickelt wurde. Allerdings war es dabei notwendig beim Sammeln und Einlösen von Punkten eine Internetverbindung zu gewährleisten, um einen Missbrauch zu verhindern. „Unser neues Protokoll garantiert nun die Privatsphäre und Sicherheit der Kunden auch im Offline-Betrieb“, sagt Andy Rupp. „Das ist wichtig für die Alltagstauglichkeit eines Zahlungssystems. Denken Sie etwa an ein U-Bahn Drehkreuz oder an Mautbrücken, dort besteht vielleicht gar keine oder nur eine zu langsame Internetverbindung.“ Alltagstauglich wird das neue Protokoll auch durch dessen eindrucksvolle Effizienz: Bei ersten Testläufen konnten die Forscher Zahlungen in etwa einer Sekunde abwickeln.

Mehr zur Forschung

Mehr zur Konferenz

Details zum KIT-Zentrum Information · Systeme · Technologien (in englischer Sprache):

Weiterer Kontakt: Martin Heidelberger, Redakteur, Tel.: +49 721 608 21169, E-Mail: martin.heidelberger@kit.edu

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 9.300 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-, Ingenieurs-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 26.000 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen.

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Diese Presseinformation ist im Internet abrufbar unter:

Weitere Informationen:

- <http://crypto.iti.kit.edu/index.php?id=cyphycrypt>
- https://homepage.ruhr-uni-bochum.de/andy.rupp/papers/bbap_ccs17.pdf
- <https://www.sigsac.org/ccs/CCS2017/agenda.html>
- <http://www.kcist.kit.edu>
- <http://www.sek.kit.edu/presse.php>

Quelle: idw

Portrait

-

News-ID: 974632 • Views: 393 (Stand: 12.08.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/974632/Sicheres-Bezahlen-ohne-Datenspur.html>