Secure Payment without Leaving a Trace

Press Release 152/2017

No matter whether payment of the public passenger transport ticket is made via a smartphone app or whether a prepaid card is used for the public swimming pool or a bonus card for the supermarket: Many people already open their "electronic purses" every day. However, most of them are not aware of the fact that by doing so, they largely lose privacy. Researchers of Karlsruhe Institute of Technology (KIT) have developed a secure and anonymous system for daily use. It will be presented at the ACM CCS 2017 conference in the USA.

Computer scientist Andy Rupp, member of the "Cryptography and Security" working group of KIT, is always surprised about lacking problem awareness: "I observed that only few users are aware of the fact that by using such bonus or payment systems they disclose in detail how and what they consume or which routes they have taken." To prevent manipulation of the accounts by dishonest users, customer data and account balances of payment and bonus systems are usually administrated with the help of a central database. In every payment transaction, the customer is identified and the details of her/his transaction are transmitted to the central database. This repeated identification process produces a data trace that might be misused by the provider or third parties.

The new "BBA+" protocol makes electronic payment secure and confidential. (Photo: Gabi Zachmann/KIT)

The cryptography expert did not want to resign himself to this apparent conflict of privacy and security. Together with Gunnar Hartung and Matthias Nagel of KIT and Max Hoffmann of Ruhr-Universität Bochum, he has now presented the basics of an "electronic purse" that works anonymously, but prevents misuse at the same time. The "black-box accumulation plus" (BBA+) protocol developed by them transfers all necessary account data to the card used or the smartphone and guarantees their confidentiality with the help of cryptographic methods. At the same time, BBA+ offers security guarantees for the operator of the bonus or payment system: The protocol guarantees a correct account balance and is mathematically constructed such that the identity of the user is disclosed as soon as the attempt is made to pay with a manipulated account.

The new protocol is a further development of an anonymous bonus card system that was also designed by the KIT research group. For collecting and redeeming points, however, it required an internet connection to prevent misuse. "Our new protocol guarantees privacy and security for customers during offline operation as well," Andy Rupp says. "This is needed for ensuring the payment system's suitability for daily use. Think of a subway turnstile or a toll bridge. There you may have no internet connection at all or it is very slow." Also its high efficiency makes the protocol suited for everyday use: During first test runs, researchers executed payments within about one second.