Secrecy obligation for the digital piggy bank

March 29 2017

With their bonus cards, consumers collect bonus points when paying for purchases. Cryptographic methods help to better protect privacy. Credit: KIT

"Do you collect bonus points?" This question is part of daily purchasing routine. More than 80% of German households participate in bonus programs. They run the risk of disclosing sensitive information about themselves, if such a system is misused. For this reason, the

Cryptography and Security Group of Karlsruhe Institute of Technology (KIT) develops a digital bonus and payment system that protects anonymity of clients, but also offers the added values desired by operators.

"Only very few consumers think about which information may be derived from their data," Andy Rupp, cryptography expert at KIT, explains. Today's systems can link every purchase and every product to personal data left by clients during their registration. And even without the explicit supply of customer data, there is a high risk of linking purchases to customer identity. The resulting movement and personal profiles allow conclusions to be drawn with respect to the purchasing behavior of people as well as to their state of health or their personal preferences.

In today's systems, the end device of the client, a smart card or a smartphone, hardly executes any calculations for bonus point collection. It only sends an identification number, by means of which the new bonus points can be allocated to a client account in the back end of the operator. Rupp and his colleague Tibor Jager from the University of Paderborn want to make these end devices more intelligent. The devices are to store the points collected themselves and to execute cryptographic algorithms together with the operator. By means of these algorithms, the points can be added or subtracted safely under protection of privacy. "This works like a digital piggy bank, whose security properties can be proved mathematically," Rupp says. Except for the customer, nobody is informed about where the bonus points come from and how many points are collected in the transactions.

Purchasing is facilitated by digital systems, but leaves distinct data tracks. Credit: KIT

"Our research is aimed at making citizens aware of the significance of privacy in the digital world," Rupp and his team say. The digital piggy bank might also be used for so-called stored-value cards, cash cards used in the public passenger transport sector. Another scenario that might become relevant in the near future is the vehicle-to-grid system (V2G). In this system, electric cars feed electricity into the public grid during times at which too little energy is available. For this, servers register the number of electric cars on parking lots as well as their capacities and coordinate the feed-in volume with the current need. The owners of the vehicle are paid a monetary compensation. In both cases, the new system is to prevent the calculation of movement profiles.

A prototype with core functions is already run on the smartphone. The team now plans to optimize it for use of smart cards and to extend its

applications. An important feature for bonus cards would be the protection of privacy. In this case, operators could calculate statistics without obtaining customer-related data.

Provided by Karlsruhe Institute of Technology