Electromobility as privacy hazard

June 3 2014

Consumers who charge an electric vehicle on a regular basis may leave a data trail. With each charging process, the system saves when and where it took place and which customer paid for it – a privacy risk, says Tilman Frosch from the Chair for Systems Security at the Ruhr-Universität Bochum (RUB). In "RUBIN", the RUB science magazine, he presents a solution designed to ensure the privacy of users' data during the charging process.

The objective: the anonymous charging station

When charging an electric vehicle, the user provides a RFID card as proof of identity at the charging station, thus transmitting personal data into the accounting system. If the customer is not anonymous and, at the same time, it is known which charging stations he has been using, this information can be used to create a movement profile. Accordingly, the RUB researchers are striving to conceal the location of the charging station when the accounting data are forwarded to the electricity supplier. However, simply leaving out this information is not an option. If, for example, a user wants to appeal against his or her invoice in court, certain location-related data, such as metre numbers, are necessary to resolve the issue.

Group signatures as solution to the problem

In order to ensure that the accounting data submitted by the charging station to the electricity supplier are correct, a digital signature is required. The IT security researchers plan to use group signature

schemes for this purpose. Such schemes mean that groups of authorised senders exist. But it is impossible to distinguish which group member, i.e. which charging station, has generated the signature. In order to be able to shed light on violations, many group signature schemes operate with a trusted third party, a so-called opener. That opener alone is able to access a certain secure part of the signature. That section contains the name of the actual group member, namely the charging station that has generated the signature.

Thinking data protection through from the outset

"Experience has shown that problems that are not identified until late, such as data trails of mobile phone users, are often rooted deeply within a technology's actual design," says Tilman Frosch. " In new technological areas such as electromobility, it is therefore vital to ensure that data security is incorporated into the design from the outset."

Provided by Ruhr-Universitaet-Bochum