Fraunhofer

PRESS RELEASE

Expert from Fraunhofer ITWM uncovers security vulnerabilities of charging stations

The infrastructure for charging electric vehicles is growing tremendously. By 2025, German automakers want at least 15 percent of their sales to be electric vehicles. Security vulnerabilities, however, plague the charging process. Mathias Dalheimer, an expert at the Fraunhofer Institute for Industrial Mathematics ITWM, warns that nearly anybody could debit charging costs to the user-friendly but insecure charging card of an unsuspecting user.

Drivers of conventional vehicles refuel at gas stations. By contrast, owners of electric vehicles use charging stations, which supply the required charging capacity. With regard to public spaces, many operators of charging stations debit costs to a user's charging card. A number stored on this card enables the charging station to identify the user. Charging costs are then deducted from the bank account linked to the card.

Unfortunately, it is easy to access and copy the ID numbers stored on charging cards. As Mathias Dalheimer explains: "It is pretty easy to clone a charging card. Many manufacturers of charging stations have failed to implement basic safety mechanisms. And because these manufacturers sell their charging stations in a number of countries, Germany is not the only one affected by this."

Charging-card number as vulnerability

Dalheimer adds that "there are insufficient safeguards for communication between charging stations and the billing back-end. Card numbers are transmitted directly to operators – often without any encryption at all. Somebody can use simple equipment to intercept these transmissions and obtain customers' card numbers. This makes it possible for criminals to forge charging cards or, what is arguably easier in practice, simply simulate charging transactions."

It would likely be very difficult for customers to prove unauthorized use of their charging cards. This is especially true of a roaming charge, when a different operator debits a customer long after charging costs are incurred. It might be weeks before anybody notices the unauthorized use of a charging-card number.

Editorial Notes
Janis Eitner | Fraunhofer-Gesellschaft, Munich | Communications | Phone +49 89 1205-1333 | presse@zv.fraunhofer.de
Ilka Blauth | Fraunhofer Institute for Thechno- und Wirtschaftsmathematik ITWM | Phone +49 631 1231600-4674 | Fraunhofer Platz 1 | 67663 Kaiserslautern | www.itwm.fraunhofer.de | presse@itwm.fraunhofer.de

Annual CCC conference emphasizes security issues of electric charging stations

In addition to working as a researcher at Fraunhofer ITWM, Mathias Dalheimer also belongs to the Chaos Computer Club (CCC). At the club's annual conference, he presented this security issue and others – which then led to detailed reports in mainstream media.

"Several operators of charging stations have acknowledged vulnerabilities; thanks to widespread media coverage, some have taken the initial necessary steps to remedy the situation," says Dalheimer. "Some large companies have already contacted Fraunhofer ITWM about making charging stations more secure. We also want to set up a consortium of experts that will systematically tackle such matters."

Security vulnerabilities plague the charging process of electric cars; unsecure charging cards can be abused. © istockphoto/Kievith (Image may only be used in connection with this press release.) | Picture in color and printing quality: www.fraunhofer.de/en/press