Cybersecurity: Plugging smart grid weaknesses

June 5 2013

Credit: AI-generated image (disclaimer)

Power companies are increasingly upgrading to smart grids—national or state-based intelligent computer systems that collect information from consumers and suppliers in order to automatically improve the grid's efficiency and reliability. The National Institute of Standards and Technology in the United States has produced a set of cybersecurity

guidelines, called NISTIR 7628, for smart grid programmers across the globe. However, Aldar Chan and Jianying Zhou at the A*STAR Institute for Infocomm Research in Singapore point out that, although the guidelines are comprehensive, they lack standardized instructions for scenarios that may arise with new technologies such as electric vehicles. Chan and Zhou have also identified two key weaknesses within NISTIR 7628.

When people plug in and charge electric vehicles, the security risks bridge the 'cyberworld' and the real world. "If there is no binding of identities between the cyber and physical domains, how can we be sure the information provided by the smart grid accurately reflects what is happening in the real world?" asks Chan. "We have little knowledge about cross-domain vulnerabilities, not to mention security mechanisms to withstand coordinated cyber–physical attacks."

Chan and Zhou examined the NISTIR 7628 framework using the scenario of a person charging an electric vehicle on a smart power grid. This framework is designed to provide a very secure system because as well as requiring a user login to pay for electricity, the car itself also needs device authentication when plugged in. In this way, a car reported as stolen would be barred from charging. Nevertheless, there may be ways of altering plug-in systems that would allow stolen vehicles to charge.

"NISTIR 7628 seems to separate cybersecurity from physical security without proper guidelines on how the two should be blended under this scenario," explains Chan. "These gaps could mean the system is open to a coordinated cyber–physical attack."

Chan and Zhou also examined the data that the smart grid system would hold. These include personal and banking details, and the physical location of the vehicle and how long it had been there—the perfect

combination for criminals to exploit.

"NISTIR 7628 takes a utility company-centric perspective here," explains Chan. "Although there is caution about consumer privacy issues involving smart meters, little attention is paid to driver privacy."

Chan and Zhou are keen to improve the NISTIR 7628 framework: "We are developing a cyber–physical authentication protocol to strengthen login security, and a protocol to balance accountability and privacy regarding the location data the smart grid can hold on individuals."

More information: Chan, A. and Zhou, J. On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. *IEEE Communications Magazine* 51, 58–65 (2013). ieeexplore.ieee.org/xpl/articl … jsp?arnumber=6400439

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: Cybersecurity: Plugging smart grid weaknesses (2013, June 5) retrieved 9 April 2024 from https://phys.org/news/2013-06-cybersecurity-smart-grid-weaknesses.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.