How safe is critical infrastructure from hacker attacks?

September 8 2017

Wind turbines often are set up in remote and uninhabited locations and therefore are hard to access. Nevertheless, our cities depend on them – increasingly so in times of the energy revolution. Credit: Roberto Schirdewahn

Critical infrastructure elements such as wind power stations are partially controlled via mobile phone networks. Using state-of-the-art tests, researchers at Horst Görtz Institute for IT-Security (HGI) in Bochum are investigating how well protected such control systems are from external attacks. The team from Ruhr-Universität Bochum has joined forces with colleagues from TU Dortmund University in the Bercom project, with the aim of making critical infrastructure in Europe able to withstand hacker attacks. A report on their research was published in Bochum's science magazine Rubin.

Outdated technology in use

As wind turbines are often scattered across large areas, they cannot be entirely controlled via cables. "Mobile telephony networks have to be used for the last mile of the control," says David Rupprecht, Ph.D. student and participant in the Bercom project. Reliable monitoring of such facilities is important to maintain control over the generated energy volumes, for example. If they are higher than the consumed energy volumes, the power grid overloads and an outage may occur. Attackers can interfere with the system by authorising surplus electricity production while overriding the system's safety measures.

"Many critical infrastructure operators currently use outdated and therefore insecure communication technologies," says Rupprecht. Those include the legacy mobile phone standard GSM. In the private sector, GSM has been overtaken by the new standard LTE.

Mobile phones rather than wind turbines

Rupprecht has developed tests for assessing how secure chipsets installed in the control units of wind turbines are. The aspects he's interested in are encryption and authentication techniques that are deployed to facilitate communication. Encryption prevents attackers from gaining access to information about the system by reading the transmitted messages. Authentication prevents attackers from sending fake commands to the control unit by passing themselves off as a real mobile phone network.

As the chipsets installed in the control units of wind power plants are identical to those used in mobile phones, David Rupprecht was able to conduct his tests using the latter. With the aid of so-called Software Defined Radios, he imitated an LTE base station that transmits signals to all mobile phones and receives signals from them in turn. Thus, he simulated attacks on different chipsets.

Inadequate encryption

The result: None of the ten tested mobile phones alerted its user to an unencrypted data exchange. When it came to authentication, on the other hand, only one phone failed the test; the other nine identified fake messages and did not authorise their reception.

In the course of the project, the researchers from Bochum and Dortmund, in collaboration with other research and industrial partners, intend to turn LTE into a more secure mobile telephony standard for the energy sector.

More information: Project website: www.bercom-project.org/

Provided by Ruhr-Universitaet-Bochum

Citation: How safe is critical infrastructure from hacker attacks? (2017, September 8) retrieved 10 April 2024 from https://phys.org/news/2017-09-safe-critical-infrastructure-hacker.html