Smart electrical grids more vulnerable to cyber attacks

August 16 2017

The potential impact of smart meter bricking attacks on fifteen of the largest U.S. metropolitan areas . Credit: Elsevier

Electricity distribution systems in the USA are gradually being modernized and transposed to smart grids, which make use of two-way communication and computer processing. This is making them increasingly vulnerable to cyber attacks. In a recent paper in Elsevier's *International Journal of Critical Infrastructure Protection*, Dr. Sujeet Shenoi and his colleagues from the Tandy School of Computer Science,

University of Tulsa, US, have analyzed these security issues. Their report provides crucial keys to ensuring the security of our power supply.

"Sophisticated cyberattacks on advanced metering infrastructures are a clear and present danger," Dr. Shenoi pointed out. Such attacks affect both customers and distribution companies and can take various forms, such as stealing customer data (allowing a burglar to determine if a residence is unoccupied, for instance), taking power from particular customers (resulting in increased power bills), disrupting the grid and denying customers power on a localized or widespread basis.

Advanced metering infrastructures can extend over a large geographic area. They consist of smart meters in homes, businesses and elsewhere (e.g. traffic lights), and meter data management systems. Data collectors act as intermediaries between the meters and the data management systems.

To assess the potential consequences of a cyber attack on an electricity meter infrastructure, Dr. Shenoi and his colleagues analyzed an advanced metering infrastructure that consists of over a million smart meters, over a hundred data collectors and two data management systems. The security analysis provides a detailed evaluation of the infrastructure's 'attack surface' (points in the system that are vulnerable to attack), targetable elements in the system (such as data collectors), and the potential attack types and their impacts.

"The most devastating scenario involves a computer worm traversing advanced metering infrastructures and permanently disabling millions of smart meters," noted Dr. Shenoi. Such attacks already occur: in December 2015, for example, the Russian hacker group Sandworm successfully attacked the Ukrainian power grid, disrupting power to more than 225,000 customers. Plant operators restored power within six hours by manually resetting the circuit breakers, but in the case of

disruption in major US cities, this would take much longer. "Damaging a few million smart meters would cause a power outage in a large geographic area that may last anything from several months to over a year," said Dr, Shenoi. This is "because of the limited production and inventories of smart meters and availability of technicians."

Advanced metering infrastructures' scale, diversity and complexity make them particularly difficult to analyze from a security perspective, but also for the utility personal to be fully trained to face such events. They are also continuously evolving in terms of scale, topology, technology (hardware, software and firmware), functionality and security controls. This makes this analysis essential to understanding the security landscape. It lays the groundwork for further research creating a framework for robust risk management programs tailored to protect individual metering systems, but also for the utility personnel to become more efficient thanks to a better comprehension of the threat environment of the new metering infrastructures.

More information: Aaron Hansen et al. Security analysis of an advanced metering infrastructure, *International Journal of Critical Infrastructure Protection* (2017). DOI: 10.1016/j.ijcip.2017.03.004

Provided by Elsevier