When hackers turn out the lights

16 September 2016

The development of the smart power grid and the smart meter in our homes to accompany it brings several benefits, such as improved delivery and more efficient billing. Conversely, any digital, connected technology also represents a security risk. Writing in the International Journal of Smart Grid and Green Communications, UK researchers explain how a malicious third party that hacked into the metering system could manipulate en masse the data being sent back to the smart grid and perhaps trigger a power generation shortfall.

Carl Chalmers, Michael Mackay and Aine MacDermott of Liverpool John Moores University, explain how the implementation of the smart grid brings many improvements over the traditional energy grid by making use of the vast interconnected infrastructure that allows two-way communication and automation throughout the entire grid, from generator to consumer and back.

"A smart grid is a complex modern electricity system which utilises sensors, monitoring, communications, and automation, to improve the electricity system," the team writes. "Smart grids fundamentally change the way in which we generate, distribute and monitor our electricity. They dramatically improve the efficiency, flexibility and reliability of the existing electricity infrastructure," they add.

The researchers point out that a critical difference between the old "passive" electricity grid and the new smart grid, is the presence of the advanced metering infrastructure (AMI) which provides the two-way communication between consumer and generator. The flow of data between consumers and generators allows the power generation companies to match demand with generation, to spot patterns in changing demand on a day to day basis or through the changing seasons and more.

However, as the UK has shifted focus from coal- and oil-fired electricity generation to being more reliant on natural gas as the fuel of choice (irrespective of wind, solar, nuclear and other alternatives), this makes the electricity grid somewhat vulnerable to accidental and incidental problems with the flow of data and to malicious manipulation for the sake of sabotage, criminal or online military/terrorist action.

The team adds that, "Critical infrastructures in particular, present a tempting target for terrorists, military strikes and hackers wanting to cause disruption, steal information or incapacitate a country remotely." The team suggests that now we are forewarned of the possible worst-case scenario with regard to the smart grid and smart meters, we must put in place security measures to protect the infrastructure and maintain that security as the hackers advance to stay at least one step ahead of the threat.

More information: Carl Chalmers et al. Securing the smart grid: threats and remediation, *International Journal of Smart Grid and Green Communications* (2016). DOI: 10.1504/IJSGGC.2016.078954

Provided by Inderscience

APA citation: When hackers turn out the lights (2016, September 16) retrieved 17 January 2021 from https://phys.org/news/2016-09-hackers.html