Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread

Elizabeth Ireland, VP Marketing, nCircle

Washington, DC and San Francisco, CA, U.S.A. --- (METERING.COM) --- April 11, 2012 - A Puerto Rico utility is believed to have lost hundreds of millions of dollars over several years as a result of the company's smart meters having been hacked, according to the KrebsOnSecurity blog.

Author Brian Krebs, referencing a 27 May 2010 FBI cyber intelligence bulletin, wrote that sometime in 2009, a Puerto Rico electric utility – believed to be the Puerto Rican Electric Power Authority (PREPA) – asked the FBI to help investigate widespread incidents of power thefts that it believed was related to its smart meter deployment. Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash – from $300 to $1,000 for residential meters and about $3,000 for commercial meters – and training others to do so.

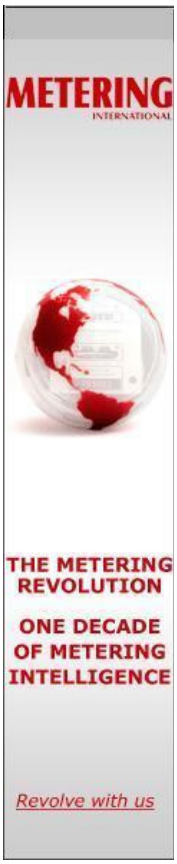
The FBI believes those responsible hacked into the smart meters using an optical converter device – such as an infrared light – connected to a laptop that allows the smart meter to communicate with the computer. After making that connection, the settings for recording power consumption were changed using software that can be downloaded from the internet. Strong magnets placed on the devices to slow the meters were also believed to being used, particularly at night, in some cases.

According to KrebsOnSecurity, the FBI said this is the first known report of criminals compromising the hi-tech meters, and that it expects this type of fraud to spread across the country as more utilities deploy smart grid technology. "The FBI assesses with medium confidence that as smart grid use continues to spread throughout the country, this type of fraud will also spread because of the ease of intrusion and the economic benefit to both the hacker and the electric customer."

A new survey by information risk and security performance management solutions provider nCircle and EnergySec indicates the view that smart meters are vulnerable to false data injection. In a survey of 104 energy security professionals, 61 percent said that smart meter installations do not have sufficient security controls to protect against false data injection.

"A false data injection attack is an example of technology advancing faster than security controls," commented Elizabeth Ireland, vice president of marketing for nCircle. "This is a problem that has been endemic in the evolution of security and it's a key reason for the significant cyber security risks we face across many facets of critical infrastructure. Installing technology without sufficient security controls presents serious risks to our power infrastructure and to every power user in the U.S."

False data injection attacks exploit the configuration of power grids by introducing arbitrary errors into state variables while bypassing existing techniques for bad measurement detection.



8 - 9 May 2012,
Bangkok, Thailand

Smart Utilities Central & Eastern Europe
15 - 16 May 2012,
Prague, Czech Republic

Metering, Billing/CRM Africa
21 - 24 May 2012,
Johannesburg, South Africa