Researchers find ways to hackproof smart meters

6 June 2019

Credit: CC0 Public Domain

Smart electricity meters are useful because they allow energy utilities to efficiently track energy use and allocate energy production. But because they're connected to a grid, they can also serve as back doors for malicious hackers.

Cybersecurity researcher Karthik Pattabiraman, an associate professor of electrical and computer engineering at UBC, recently developed an automated program aimed at improving the security of these devices and boosting security in the smart grid.

"Our program uses two detection methods for these types of attacks. First, we created a virtual model of the smart meter and represented how attacks can be carried out against it. This is what we call design-level analysis. Second, we performed code-level analysis. That means probing the smart meter's code for vulnerabilities, launching a variety of attacks on these vulnerabilities," said Pattabiraman.

The method, described here, addresses smart meters' vulnerability to what the researchers call software-interference attacks, where the attacker physically accesses the meter and modifies its communication interfaces or reboots it. As a result, the meter is unable to send data to the grid, or it keeps sending data when it shouldn't, or performs other actions it wouldn't normally do.

Pattabiraman and his co-author and former Ph.D. student, Farid Tabrizi, also found that although both techniques successfully discovered attacks against the system, code-level analysis was both more efficient and more accurate than design-level analysis. Code-level analysis found nine different types of attacks within an hour, while design-level analysis found only three. All of the attacks can be carried out by an attacker with relatively low cost-equipment purchased for less than $50 online, and do not require specialized expertise.

"Smart meters are critical components of the smart grid, sometimes called the Internet of Things, with more than 588 million units projected to be installed worldwide by 2022," added Pattabiraman. "In a single household you can have multiple smart devices connected to electricity through a smart meter. If someone took over that meter, they could deactivate your alarm system, see how much energy you're using, or can rack up your bill. In 2009, to cite one real-life example, a massive hack of smart meters in Puerto Rico led to widespread power thefts and numerous fraudulent bills."

Hacked meters can even cause house fires and explosions or even a widespread blackout. Unlike remote servers, smart meters can be relatively easily accessed by attackers, so each smart meter must be quite hackproof and resilient in the field.

The researchers say vendors can use the findings to test their designs before they are manufactured, so they can build in security from the get-go. This can make smart meters much harder to crack. By

using both approaches—design-level and code-level—vendors can guard against software tampering on two different levels.

"Our findings can be applied to other kinds of devices connected to a smart grid as well, and that's important because our homes and offices are increasingly more interconnected through our devices," said Pattabiraman.

He adds that as with all security techniques, there is no such thing as 100 per cent protection: "Security is a cat-and-mouse game between the attacker and the defender, and our goal is to make it more difficult to launch the attacks. I believe the fact that our techniques were able to find not just one or two vulnerabilities, but a whole series of them, makes them a great starting point for defending against attacks."

More information: Farid Molazem Tabrizi et al, Design-Level and Code-Level Security Analysis of IoT Devices, *ACM Transactions on Embedded Computing Systems* (2019). DOI: 10.1145/3310353

Provided by University of British Columbia