The 2019 General Meeting and PIESA-IERE South Africa Forum
October 28-31, 2019

Security Testing for Preventing Backdoor Threat in Smart meter Implementation In Indonesia

Mukhamad Faiz Fanani
IT Security Analyst, PLN
Jakarta, Indonesia

Astri Kartika
IT Strategy Manager, PLN
Jakarta, Indonesia

Keywords: *(smart meter, backdoor, whitebox firmware testing)*

Abstract

Indonesia's state-owned electricity company, PLN currently uses Automatic Meter Reading system (AMR) for large customers and plans to implement Advanced Metering Infrastructure (AMI) using smart meter for small-scale customers (households). The use of AMR technology can cause security issues and probability increases in line with the number of meter installed. One of the security issues is the existence of a backdoor on the smart meter firmware.

Backdoor is a method or function embedded by an attacker into the internal structure of the firmware meter so that the attacker can make full access to the meter system without going through legal authentication and authorization mechanisms. Backdoor can also materialized in form of a special function made by meter manufacturer called factory login function. The existance of backdoor is used for many purposes, one of them are for gaining billing information or reset meter data. This study will propose and asses security testing method to detect backdoor threat in smart meter implementation in Indonesia. Current testing method that only focus on functionality and durability are considered not sufficient to detect and prevent backdoor threats contained in the internal meter firmware.

This study propose an additional testing to detect and prevent backdoor threat. The security testing proposed is called Whitebox Firmware Testing. Whitebox testing is done by checking the internal firmware meter system. Checking the internal meter system is done before the firmware is installed into the meter. However, considering the time required for testing due to number of codes that may reach hundred thousands, the testing method proposed is by checking each method or function contained in the internal firmware. The tester must ensure that in the firmware meter, there are no other methods or functions in the firmware other than those already defined in the firmware design document. The examiner also checks every function / method that represents the features of the meter and ensures that the feature runs according to its function. After being declared appropriate and there is no backdoor or malicious function embedded in the firmware, the tester generates a checksum or hash code from the firmware to ensure that the firmware that has been tested by the whitebox is not changed again without the examiner's knowledge. The benefit expected from this security testing is any potential backdoor may be detected earlier, thus reduce the possibility of security threat when smart meter is already installed on the field.