# Security Risks Evaluation Toolbox for Smart Grid Devices

Yang Liu, Jiahe Liu, Ting Liu, Xiaohong Guan, Yanan Sun
Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an, Shaanxi, China
{yliu, jhliu, tliu, xhguan, ynsun}@sei.xjtu.edu.cn

## ABSTRACT

Numerous smart devices are deployed in smart grid for state measurement, decision-making and remote control. The security issues of smart devices attract more and more attention. In our work, the communication protocol, storage mechanism and authentication of smart devices are analyzed and a toolbox is developed to evaluate the security risks of smart devices. In this demo, our toolbox is applied to scan 3 smart meters/power monitor systems. A potential risk list is generated and the vulnerabilities are further verified.

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection*

## General Terms

Security

## Keywords

Smart Grid, Smart device, Security risk evaluation

## 1. INTRODUCTION

In smart grid (SG), various smart devices are deployed into power systems to provide a desirable infrastructure for real-time measurement, transmission, decision and control. At the same time, numerous widely-deployed smart devices provide the attackers a great opportunity to attack SG. Various attacks such as eavesdropping, information tampering and malicious control command injection that have almost ruined the Internet, would impose serious threat on secure and stable SG operation. In our work, we found many common security risks could be easily implemented on the smart devices.

**Bad Data Injection (BDI):** The attackers may inject bad data into SG through tampering meter's data. Moreover, the large scale BDI attack [3, 5] may lead the control center's making the wrong decisions and sending false commands.

**Privacy Leakage:** The malicious users can access the smart devices to obtain the privacy of the users. For example, the behaviors of users and appliances could be identified from the power load profile, using nonintrusive load monitoring system (NILMs) [2, 4].

**Cyber Attacks:** In recent years, various cyber attacks have been implemented into SG, such as smart meter worm [1], meter botnet, DoS, fabricating authentication, Session Hijack, and so on. In 2010, the Stuxnet worm attacked the Iran's Bushehr nuclear plant and damaged lots of centrifuges.

At the same time, it is a huge challenge to prevent these security risks, because: 1) it is almost impossible to monitor all smart devices, since numerous devices are widely deployed in the SG; 2) the computation power and storage space of most smart devices are limited to implement common security defense system.

In our work, the communication protocol, storage mechanism and authentication of smart devices are investigated. Lots of vulnerabilities are found and collected, which would cause serious attacks on smart devices, such as password cracking, authentication bypassing, user's privacy leak, bad data/false command injection and so on. A toolbox is developed to evaluate the security risks of smart devices. In present demo, the toolbox is applied to scan 3 smart meters/power monitor systems. A potential risk list is generated and the vulnerabilities are further verified.

## 2. DESIGN AND IMPLEMENT

As shown in fig. 1, the toolbox is developed on the Android 4.1, consisting of two parts: 1) a database is developed to recode the communication protocols, storage structure, vulnerability & exploiting method, and authentication of smart devices; 2) an open function platform is provided to integrate various risk evaluation and verification function module.

### 2.1 Configuration and Risk Database

**Communication Protocol:** Most smart meters adopt standard protocols in industry, such as Modbus and DNP3.0. IP based protocols are regarded to be the future trend due to its high data transfer rate, robustness and fine fault tolerance. In this demo, the Modbus is applied.

**Storage Structure:** In most smart devices, the real-time log data are stored in memory, and system parameters and all historical log data are stored in NVRAM. A register map is established to map the data to the register. In our work, we analyze the data storage structure are generate the reg-


*SIGCOMM* '13, Aug 12-16 2013, Hong Kong, China.
ACM 978-1-4503-2056-6/13/08
http://dx.doi.org/10.1145/2486001.2491693.

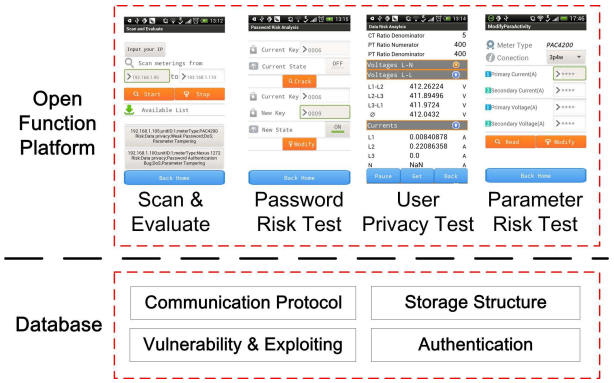


**Figure 1: Structure of Toolbox**

ister map, by analyzing the handbook and communication traffic.

**Authentication Mechanism:** The authentication is adopted in smart devices to prevent the invalid users. However, we found most of them are derived from the industrial control systems which focus on the reliability, real-time and cost, with little regard for information security. In our work, many authentication mechanisms are collected and analyzed to find whether the invalid users can access the smart devices.

**Vulnerabilities and Exploiting:** In the above investigations, lots of vulnerabilities in smart devices are found. `Denial-of-Service (DoS):` It is easy to launch a DoS attack against smart device, since the service capability and security defense ability of the smart devices are limited. For example, one famous smart meter can support 13 TCP conversations and has not any mechanism to detect and disconnect duplicate links. When a hacker has created 13 conversations with this meter, any new request from valid users will be denied. `Weak Password:` The passwords of many smart meters are incredible weak, considering the password length or charsets, resulting in authentication failure. For example, one smart meter's password is only composed of 4 digits. And most meters have no mechanisms to prevent from vicious password attempts, so it can be cracked easily by brute force. Moreover, the power readings on smart meters would cause user privacy leakage; the attackers can tamper the parameters to refuse valid user access or lead data inconsistent problems; the hackers can bypass the authentication to access the devices exploiting the forged identity.

## 2.2 Open Function Platform

The toolbox is developed on Android 4.1 platform. In present version, there are four function modules:

**Scan and Evaluation Module** is used to scan specified network and find out all the online smart meters. A list of the basic configuration information and risks evaluation result for each online device is provided.

**Password Risk Test Module** is applied test the risk of password exploiting various methods, including brute force of weak password and bypassing authentication, etc.

**User Privacy Test Module** is developed to obtain the device readings via sending data query requests. Moreover, it can detect the change of measurement and predict the user behaviors.

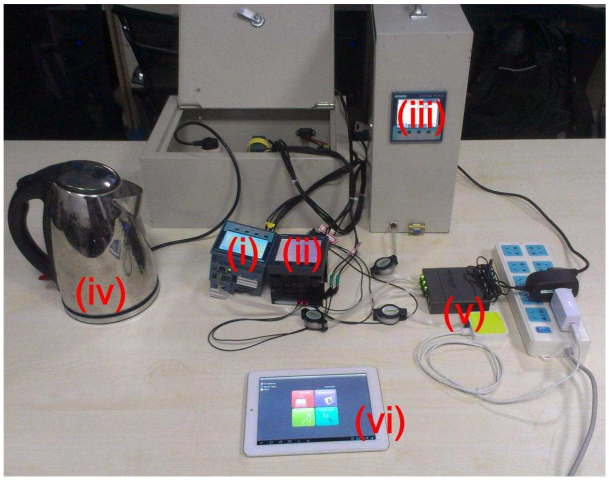


**Figure 2: Mobile Micro Smart Grid System**

**Parameter Risk Test Module** is designed to modify various parameters on devices, such as name, IP address, time, System Hookup, current transformer Ratios (in smart meter), etc.

# 3. DEMONSTRATION SETUP

We setup a mobile micro smart grid system, as shown in Figure 2. Three common smart meters/power monitor systems (i) – (iii) are deployed to measure the power consumption of an electric kettle (iv) and the routers (v), which are connected in the same network. An Android tablet (vi), installed the Security Risks Evaluation Toolbox, is used to scan the devices in this micro smart grid and evaluate the risk of three smart meters. All potential risks could be further verified accessing the smart meters.

**Acknowledgments** This project is supported in parts by a gift fund from the Cisco URP, Doctoral Fund of Ministry of Education (20110201120010), NSFC (91118005, 91218301, 61221063, 61203174) and the Fundamental Research Funds for the Central Universities.

# 4. REFERENCES

[1] M. Davis. Smartgrid device security: Adventures in a new medium. *Black Hat USA*, 2009.

[2] S. Drenker and A. Kader. Nonintrusive monitoring of electric loads. *Computer Applications in Power, IEEE*, 12(4):47–51, 1999.

[3] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 21–32, Chicago, Illinois, USA, 2009. ACM.

[4] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid. *Security & Privacy, IEEE*, 7(3):75–77, 2009.

[5] L. Ting, G. Yun, W. Dai, G. Yuhong, and G. Xiaohong. A novel method to detect bad data injection attack in smart grid. In *Proceedings of 2013 IEEE INFOCOM, Workshop on Communications and Control for Smart Energy Systems*, pages 2594–3589, Turin, Italy, 2013. IEEE.