Collusion and fraud detection on electronic energy meters: a use case of forensics investigation procedures

Rubens Alexandre de Faria, Keiko V. Ono Fonseca and Bertoldo Schneider Jr.
Department of Electronics
Federal University of Technology Parana (UTFPR)
Curitiba, Brazil
rubens@utfpr.edu.br

Sing Kiong Nguang
Department of Electrical and Computer Engineering
The University of Auckland, Auckland, New Zealand
sk.nguang@auckland.ac.nz

Abstract— **Smart meters (gas, electricity, water, etc.) play a fundamental role on the implementation of the Smart Grid concept. Nevertheless, the rollout of smart meters needed to achieve the foreseen benefits of the integrated network of devices is still slow. Among the reasons for the slower pace is the lack of trust on electronic devices and new kinds of frauds based on clever tampering and collusion. These facts have been challenging service providers and imposing great revenues losses. This paper presents a use case of forensics investigation procedures applied to detect electricity theft based on tampered electronic devices. The collusion fraud draw our attention for the involved amounts (losses) caused to the provider and the technique applied to hide fraud evidences.**

Index Terms—electronic meter, electricity measurement fraud, tampering technique, forensics investigation procedure

I. INTRODUCTION

Electricity theft is not a new problem for energy utilities. In Brazil, non-technical losses caused by electricity theft can be as high as 20% of the generated energy delivered to the distribution network [1]. All Brazilian energy utilities suffer from theft losses. This scenario is not restricted to underdeveloped countries: the percentage varies and occurs in almost all countries [2]. Among the usual fraud techniques are illegal tap wiring and meter tampering through security seal violations. These frauds are detected by periodical line inspections and fraud evidences are easily found, allowing thieves prosecutions [3].

Energy providers are constantly challenged to uncover new fraud techniques developed by creative people, for example, collusion and scams [4]. Fraud techniques keep evolving: electronic meter with bi-directional communication provides new vulnerabilities to interconnected systems. New subtle fraud techniques are surprisingly refined by the knowledge applied to energy stealing as well as the amount of damages. These facts pose high level countermeasures and systematic forensics investigation for detecting fraud and evidence gathering.

Quite disturbing was the recent unveiling of many tampered devices in middle-size industries at South Brazil, with associated revenue losses of U$1,000,000 to the energy utility in less than a year. The applied technique was undetectable by usual anti-fraud inspection techniques: it was detected by chance due to an assembling failure in one of the tampered devices. The fraudsters circumvent the security sealing violation, avoiding tamper violation sensors and making the meter tampering invisible to the naked eyes.

In our paper we describe details of the referred technique; the investigation steps followed to evidence gathering and discuss possible countermeasures to avoid similar fraud attempts under the light of the Smart Grid context.

Authors are with the Federal University of Technology – Paraná, campus Curitiba (+55-41-33104616; e-mail: rubens@utfpr.edu.br).

II. CONTEXT

In Brazil, most residential consumers have their electricity consumption measured on a monthly basis by checking a meter placed at their premises. This *in loco* procedure requires the energy utility to hire subcontractors or keep personal especially hired to meter reading [5]. A Electro-mechanical Meter [6] is usually installed at the residential consumer, outside the main house inside a metallic shelter, protected from rain, and its display should be accessible for a local reader [7] to show the accumulated value (total amount) of energy consumption. Usually power factor or instantaneous consumption samples can not be directly read from the meter.

Electronic meters [7] are mostly intended to consumers adopting time-based pricing tariff (also known as time-of-use or TOU pricing) or with special requirements of energy quality for example, those of large-scale energy consumers. The electronic meter can be featured to meter energy consumption associated to a particular time period (TOU), active and reactive power, power factor, distortion power and can also present several other metering information, for example, number of energy supply interruptions, interruption period, time stamp of interruptions [9][10][11]. They can also be featured to provide bi-directional communication aiming at providing periodical or sporadic event reports as well as receive remote commands from the energy supplier. We recall that energy price varies to large-scale energy consumers not only on a provider basis but also on TOU period: at peak-period (Monday to Friday, 18:00h - 21:00h) the kWh price can be up to 50% higher than another time schedule [12].

DOI 10.1109/SPW.2014.19

Tampering of electromechanical meters is not uncommon for fraud goals (under-registering) through security seal violation and direct or indirect changes to the mechanical disc. The same is not easily accomplished on electronic meters: built-in sensors are used to report meter tampering, security sealing violation, wiring changes, magnetic anomalies, switched phases, abnormal clock settings, etc..

III. A VULNERABILITY POINT UNVEILED

We describe here a case of electricity theft detected at a particular utility in South Brazil. This utility installs an electronic meter to its large-scale energy consumer with a verification block (also known as "Switch Block", hereafter denoted as SB) attached to it [13]. Figure 2 shows a typical SB circuit used to derive or isolate the meter for maintenance or calibration services: a set of 3 single switches (connected to voltage sensors, one for each phase) and 3 twin switches (a twin switch for each of 3 current sensors, one for each phase). The schematic diagram shows the switches in parallel to the meter voltage and current sensors. SB Switches should remain open all the time except for maintenance [14].

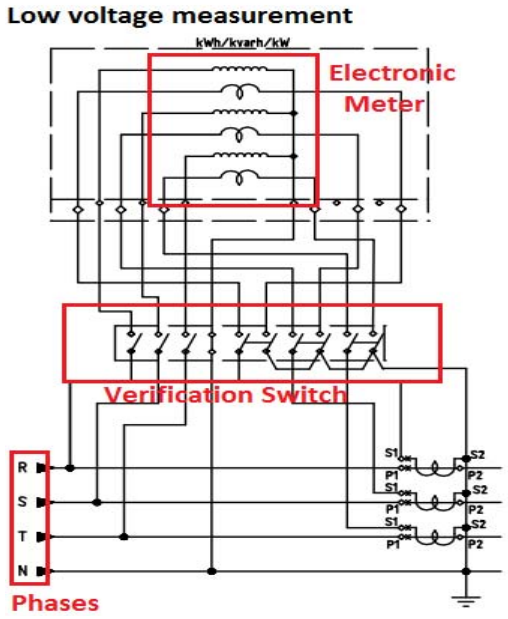

Figure 2 –Diagram of an electronic meter connected to a SB [14].

The SB is typically assembled in a box with a transparent removable front, secured sealed by the distribution utility (traceable sealing wax) and protected against non-authorized access. Figure 3 shows the open SB block case at 3A (top view) and the bottom view at 3B [15].

The maintenance procedure requires authorized personal to break the SB sealing wax, to remove the transparent front and to turn the switches to the ON position short-circuiting the sensor lines. The SB operation disconnects the meter without interrupting the electricity flow to the consumer. During the maintenance (just a few minutes), the energy consumption is not measured. After the maintenance, switches are turned off, the box is closed and a new sealing wax is placed. This is a standard maintenance procedure for large-scale energy consumers [14].

This particular testing block turns out to be a vulnerable point on the billing process as explained at the next section.

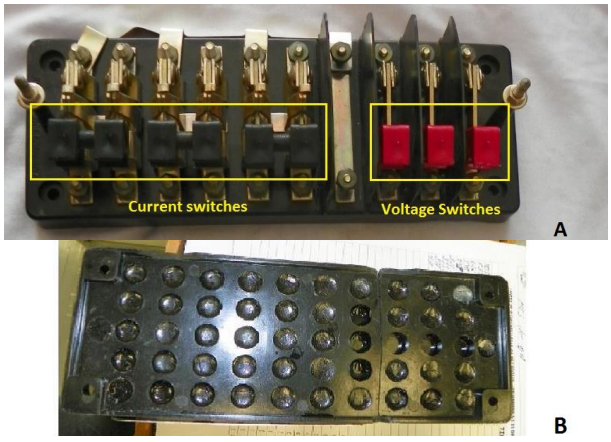

Figure 3 –Verification Block (A) Top view (B) bottom view [15]

IV. THE FRAUD EVIDENCES

In order to reduce energy costs, some industries, mainly those of 24/7 uninterrupted operations, have their own power generators (thermoelectric generators) to avoid buying utility energy at the peak period (most expensive period). Coincidently, within a same geographical region (radius of 50km among cities in south Brazil), circa of 10 medium-size industries had their energy consumption clearly reduced on a short period of time (two months).

Once significant differences of energy consumption along the time are detected, the utility carried out an investigation by remote monitoring (telemetry) the metering device. Remote reading and record analysis of the aforementioned region reported no electrical current and normal voltage values at all 3 phases over some time periods. These values are usual if associated to the use of consumer´s own generators at the particular measurement period. However, the utility load balance was inconsistent: power generation did not match the measurement of power consumption, reporting significant power system losses. The energy distribution team carefully checked all lines fed by the generator at likely lossy branches but could not find abnormal situations [10][11].

Finally, 2 months after the energy deficit findings, a routine telemetry analysis of one consumer showed strange measurement values: 2 phases presented null current but constant and normal voltage values but one phase presented not null current consumption but null voltage. This atypical situation is very unlikely to occur, possibly due to an unusual problem on a voltage sensor inside the meter. Further analysis also found out that measurements presented usual values at some time intervals, suggesting an intermittent defective behavior of the meter.

A maintenance team went to the consumer and replaced the faulty meter and the SB. Lab tests revealed non-compatible electrical measurements at the SB, although apparently no violation of the security sealing or device case were visible. After breaking the bottom of the SB case, other than switches were found hidden under the epoxy resin as showed at Figure 4. Non-original electronic devices installed to the original SB device lead to a crime report of device adulteration. A criminal investigation had begun to ascertain a suspicion about energy theft [16].

Figure 4 – The verification switch and abnormal electronic devices hidden under the epoxy resin [15]

The scientific police team carefully managed to remove the epoxy resin to unveil the electronic circuit configuration and its purposes. The electronic device turned out to be a printed circuit board with a microcontroller and a RF receiver showed at Figure 5.

Figure 5 – Printed circuit board with a PIC 12C508A microcontroller and a RF receiver model RXTCH10 [15].

The PIC 12C508A microcontroller [17] has an 8 bits bus; less than 1kB memory size for program; 25 bytes of RAM; serial port interface and 6 I/O pins. The I/O pins were connected through current buffers and command the triggering of 250V/10A electromechanical relays. The microcontroller serial interface (RX pin) was connected to a circuit board of a RF receiver (RXTCH10 model [18], 433.92MHz RF carrier). The relays were directly connected to the SB contacts. A remote command to the microcontroller can be received by the RF receiver. The microcontroller can send current to current drivers and through the relays the SB switches can be closed. That is, the RF command sets a bypass of the current sensors of the electronic meter. The investigation concluded that a RF transmitter could send the aforementioned command. Such transmitter can be easily adapted from those available to house applications (gates control, etc.) or alarm devices. The transmission range of these devices is around 150 m.

Following the discovery of the first tampered SB unit, the police extended its investigations and together with the utility technical team found out four more suspicious equipment installed at large-scale energy consumers within the same region. Figures 6 and 7 show other devices found out inside SB units. The adulteration approach was quite similar with some minor differences (radio and microcontroller).

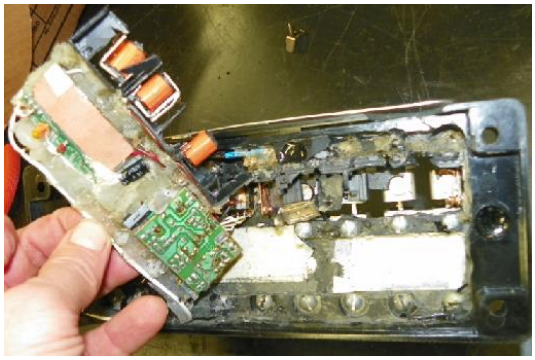

Figure 6– Printed circuit boards inside an tampered SB unit

Figure 7 shows a microcontroller not soldered on a printed circuit board (just “wired up”). Although a very amateur built-in circuit, it was efficiently applied to accomplish the fraud.

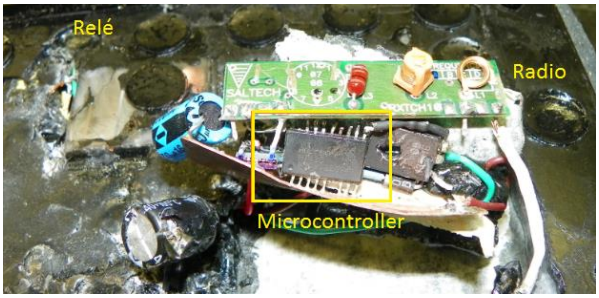

Figure 7 – printed circuit board and wire-up circuit removed from the epoxy resin

V. PROCESSING THE PHYSICAL EVIDENCES

Using a common RF transmitter and a spectrum analyzer, we established the exact transmission frequency used to command the relays to turn on the SB switches. A remote command is transmitted to the RF receiver inside the SB unit and the relays are triggered to set short-circuits of the meter current sensors.

The evidences associated to telemetry logs [19] led the police and the utility to the same conclusion after analyzing current measurements and relating them to the removal of the tampered equipment: (1) before and (2) after the removal. Figure 8 shows both situations: (1) in red and (2) in blue.

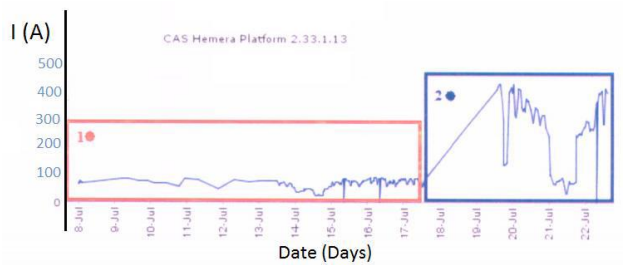

Figure 8– Screenshot of utility supervisory software showing current consumption in one phase before(1) and after(2) the tampered unit removal.

Considering data related to the Figure 8, 5 days before the meter replacement (interval 1 in red) the current consumption is less than 100A/phase and mostly uniform along 24 hours of the day. After removing the tampered device, current consumption greatly varied in time leading to an average consumption of 300 to 400A/phase in 10 days (interval 2 in blue). The peak consumption differences set behavior patterns related to non-uniform workloads or changes of the power source to thermo electrical generators.

By checking similar behaviors at other large-scale energy consumers within the same region, the utility was able to detect more tampered devices. The data analysis could have prevented the frauds if automated analysis by using some computational intelligence over historical data were used.

VI. THE PHYSICAL EVIDENCES AND THE AMOUNT OF LOSSES

Although data related to the power balance correctly pointed out the losses, the fraud was only detected by chance due to a circuit wiring error in one SB attached to a meter. The wiring error was a wrong soldering of one relay to the voltage derivation instead of one current phase switch.

Considering only the Figure 8, a simple analysis of the amount of losses reveals the scale of the fraud: the increase of 200% on the energy consumption measured after the tampered equipment removal; 3 phases; 5 fraudsters and 6 months of fraud, leads to a million dollars related to energy theft. We did not take into account the higher energy price during peak periods just the standard period price. Thus, the amount is a lower bound of a rough estimation.

Unfortunately, not all telemetry logs could be used as evidences: some were corrupted or not properly captured or stored. Based on this reason we firmly believe the amount of losses caused by this kind of tampering could be bigger and maybe still undetected in other Brazilian regions.

VII. CONCLUSION

Frauds on electricity measurement systems are not limited to underdeveloped countries. The concern is not the unlawful act but the increasing number of committed crimes with advanced technologies and sophisticated methods.

We highlight the fact that relying only on the traceable sealing wax is not enough to prevent or restrain modern criminals. The cross-border organized crime has now qualified staff: the reported fraud required personal able to build an epoxy resin case that mimic the one provided by the utility, build electronic devices, do equipment violation without breaking security sealing or letting visible traces.

In Brazil, non-technical losses urge an intelligent approach to minimize security problems of critical infrastructures: in 2012 a federal regulation sets 2014 as the beginning year for the rollout of electronic meters at residential consumers [20]. The new metering device is aimed at providing functionalities required to Smart Grids such as TOU, energy quality information, energy demanded/provided to the grid.

The Smart Grid concept relies on integrated systems of automated metering, control systems and computational intelligence based on actual and real time data about power generation and demand. The new challenges for securing and protecting companies and consumer assets require special expertise on data analysis and security requirements engineering methods.

ACKNOWLEDGMENT

Authors thank the National Council for Scientific and Technological Development (*CNPq*) for the financial support.

REFERENCES

[1] K. V O Fonseca et al: Data security issues on metering systems of energy consumption in Brazil, Espaço Energia, issue 18, 2013.
[2] ANEEL – National Agency of Electrical Energy, Technical Note 228/2013 (in Portuguese), July 2013.
[3] Jurisprudência Brasil, Security sealing violation of electronic meters (in Portuguese), available in http://www.jusbrasil.com.br/topicos/1383854/violacao-de-lacres-de-medidores-de-energia-eletrica, accessed in November/2013
[4] J. McCullough: Deterrent and detection of smart grid meter tampering and theft of electricity, water, or gas, available at: http://www.elstersolutions.com/en/deterrent-and-detection-of-smart-grid-meter-tampering-and-theft, accessed in February/2014
[5] ANEEL - National Agency of Electrical Energy, Procedures for Electrical Energy Distribution at National Electrical System (in Portuguese), PRODIST Mod.5, Measurement System, 2008.
[6] Smart Grids and Electromechanical Meters (in Portuguese), available in http://www.redeinteligente.com/2011/01/24/brasileiro-ainda-nao-pode-escolher-fornecedor-de-energia-eletrica/,accessed in 01/02/2014.
[7] Personal files, Electronic meter arrested by Scientific Police of Parana, March 2013.
[8] COPEL, ETC 2.03 (in Portuguese), Technical Specification. Edge measurements on closed environments, December 2005.
[9] COPEL (2), ETC 4.06 (in Portuguese) – Technical Specification of Multifunction Meters, September 2012.
[10] COPEL (3), ETC 4.05(in Portuguese)– Technical Specification of electronic Meters 30(200)A, July, 2013.
[11] COPEL (4), ETC 4.09 (in Portuguese), –Technical Specification of electronic meter for billing and energy quality purposes, July 2011.
[12] ANEEL (2), Resolução Homolog. 1565 (in Portuguese), July/2013.
[13] COPEL (5), ETC 2.02 –Technical Specs. of Switch Blocks, 01/2013.
[14] COPEL, Technical Standards, Distribution of Primary voltage provision, NTC 903100, October2013.
[15] Personal files, Image of Switching Block arrested by Scientific Police of Parana, March, 2013.
[16] Código Penal Brasileiro, article 155, Law Decree Nº 2.848, 7/12/1940
[17] Microchip, datasheet PIC 12C508A, available in http://www.microchip.com, accessed in 10/07/2013
[18] Holy Stone Enterprise Co, datasheet ASK Receiver Module, V2.0
[19] Personal files, Database of Electricity Operation Supervisor, Scientific Police of Parana, March, 2013.
[20] ANEEL-National Agency of Electrical Energy: RN502 (in Portuguese), 07/08/2012