The Most Frequent Energy Theft Techniques and Hazards in Present Power Energy Consumption

Robert Czechowski - Wroclaw University of Technology, Poland

Anna Magdalena Kosek - Denmarks Tekniske Universitet, Denmark

April 12th 2016

Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG2016)

This presentation was realized within NCBR project: ERA-NET, No 1/ SMARTGRIDS/2014, acronym SALVAGE: *Cyber-Physical Security for the Low-Voltage Grids.*

Wroclaw University of Technology

DTU Danmarks Tekniske Universitet

Agenda:

1. Electricity crime,
2. The main reasons for electric energy theft and consequences,
3. Classification of electric energy theft,
4. Popular methods,
5. Security mechanisms,
6. Methods of energy theft detection,
7. Read Flash Chips,
8. Reverse engineering**,**
9. Smart Meter Data Analisis,
10. Energy theft on The World.

In this June 13 file photo, an electrical linesman repairs cables in the middle of a spider web of illegal subsidiary wires around the main cables in Allahabad, India. Stealing of power is a frequent phenomenon in Indian towns. AP Photo by Rajesh Kumar Singh.

1. Electricity crime:

The Penal Code considers this practice a crime punishable by imprisonment of **3 months to 5 years** (in Poland), **minimum 350 EUR fine and up to 18 months in prison** (in Denmark), up to six months or a fine of up punishing to 360 daily rates or if value exceeds **2 000 EUR**, is punished with imprisonment up to three years, who extracts energy worth more than **40 000 EUR**, to be punished with imprisonment of one to ten years (in Austria).

Electricity Theft: A Bigger Issue Than You Think ▶

2. The main reasons for electric energy theft and consequences

The main motive is desire to save money.

1. Safety…
2. Economy…
3. Society…

As electric energy suppliers inform us, the ingenuity of so-called clients knows no boundaries. Based on their many years of experience, they assure us that there are…

about 300 different theft techniques.

3. Classyfication of of electric energy theft

Issues related to energy theft can be presented in the following categories:

1 - **classic energy theft** from a line in front of the meter,

2 - **modification of the meter's operation** - short circuiting or terminal modification and tampering with the physical security mechanisms of the meter,

3 - **modification of the meter's memory**- tampering with the memory and motherboard chip of the meter.

4. Popular methods

The most important and most popular theft techniques are:

1 - hidden connection in front of the meter,

2 - physical tampering with the terminals or bridging,

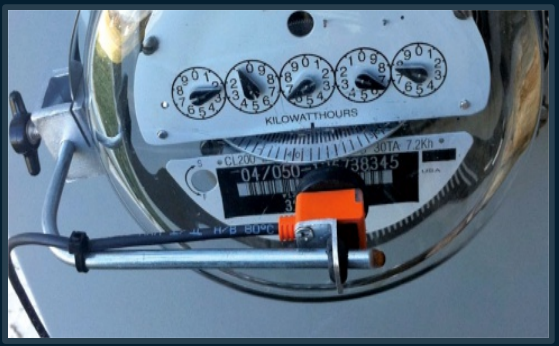
3 - tampering with a digital meter’s software,

4 - physical tampering with an analog meter’s mechanism:

magnetic field, ►

photographic film,

housing drilling.



5. Security mechanisms

Physical security of energy metres:

1 - physical security measures,

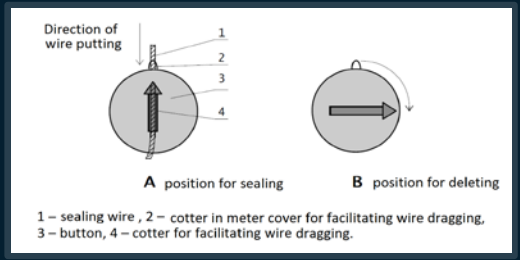
2 - physical parameterization switch,

3 - motherboard construction,

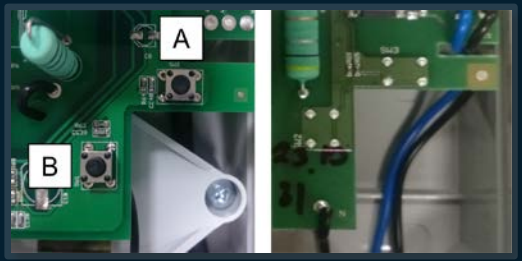
4 - magnetic field detector,

5 - HASP key (software security),

6 - communication encryption.



View knob with sealing way (large-display mode - position A, mode parameter - position B).



The view of button recording parameter setting (on the left with option, on the right hardware version without options).

6. Methods of energy theft detection

The most popular methods include:

1 - a method based on calculating the balance difference,

2 - control meter method (traditional),

3 - roaming balance meter method,

4 - reflectometer testing - (using the wave effect),

5 - provoking method,

6 - confidential phone call.

7. Read Flash Chips

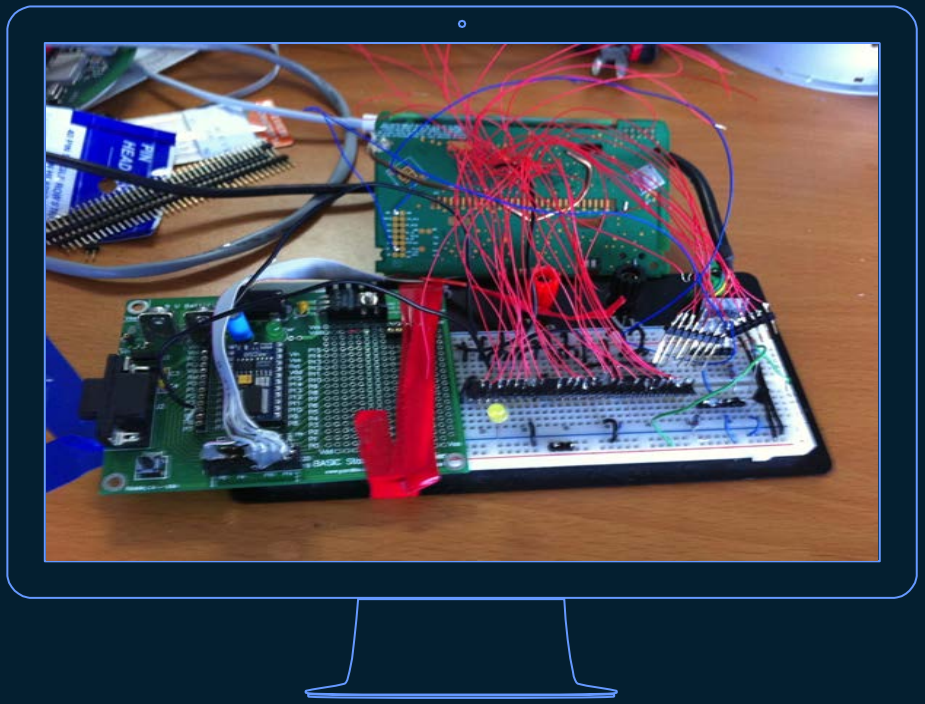
Serial EEPROM:

1. from the datasheet identify SPI pins,
2. configure the Aardvark EEPROM Board,
3. use FlashCenter to read flash memory.

IOActive

Source: *K. Shaw, Smart Meter Hardware Hacking Class, IOActive training course, IOActive Hardware Software, Wetware - Security Services, 2015.*

8. Reverse engineering

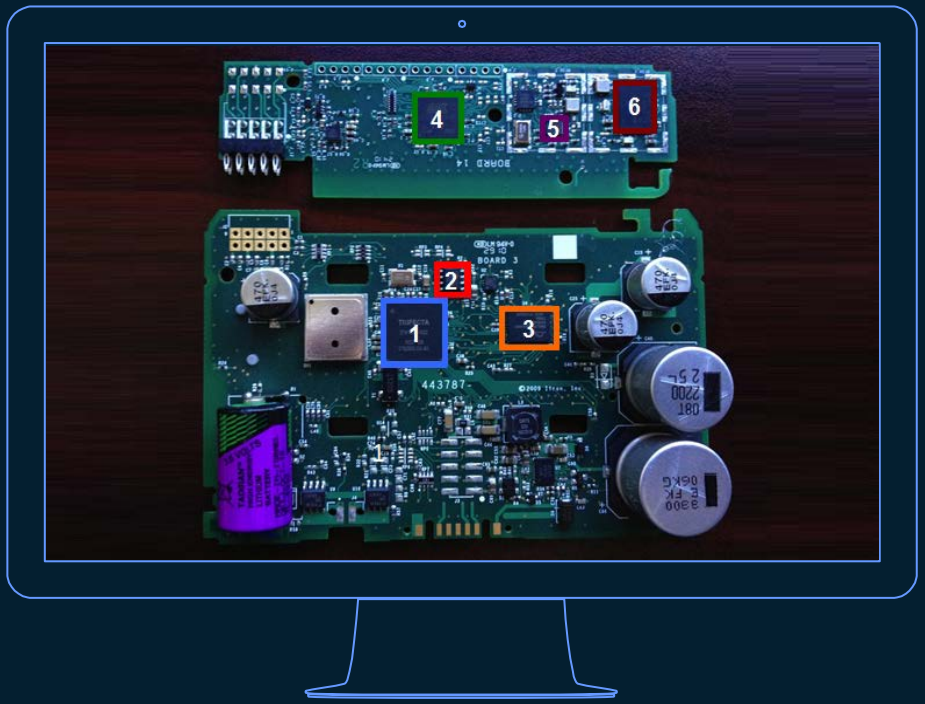


View of Smart Metering mainboard during reverse engineering.

IOActive

Source: *K. Shaw, Smart Meter Hardware Hacking Class, IOActive training course, IOActive Hardware Software, Wetware - Security Services, 2015.*

8. Reverse engineering



Example motherboard of Smart Meter with marked chips: 1 – Trifecta (Register, LCD Driver, Zigbee), 2 – ATMEL (EEPROM), 3 – Spansion (Flash), 4 – ATMEL AT91SAM7 (Communications), 5 – CC1101, 6 – Skyworks.

IOActive

Source: *K. Shaw, Smart Meter Hardware Hacking Class, IOActive training course, IOActive Hardware Software, Wetware - Security Services, 2015.*

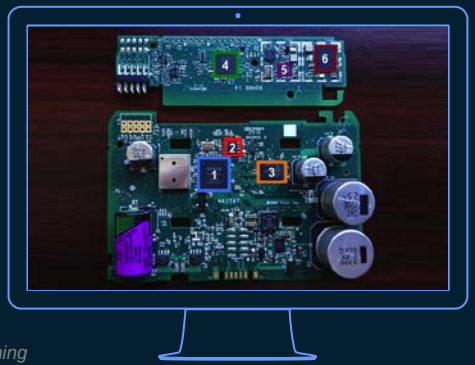
8. Reverse engineering

READ FLASH CHIPS

- Spansion BGA Flash:
  1. Remove all existing solder
  2. Apply a thin layer of liquid flux
  3. Use mask to add solder balls
  4. Use hot air station to melt solder balls
  5. Remove messed up balls
  6. Fixup with soldering iron
  7. Place in SuperPro 5000
  8. Read flash

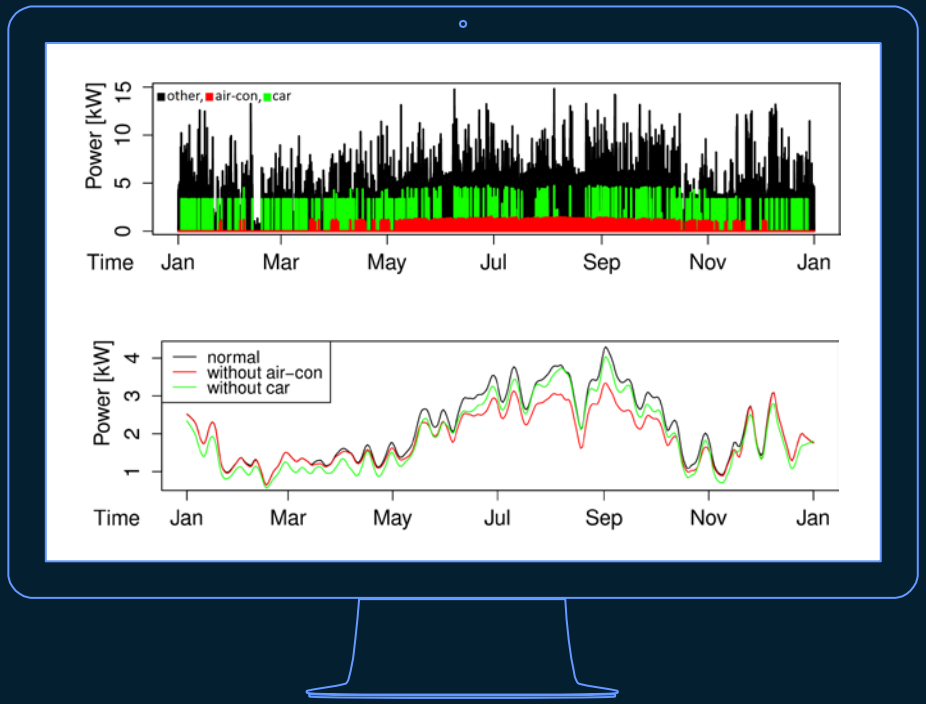
WARNING!
Very
Tedious
(Best not to attempt)

View of connections a bunch of lines to the villas on the back of the meter…



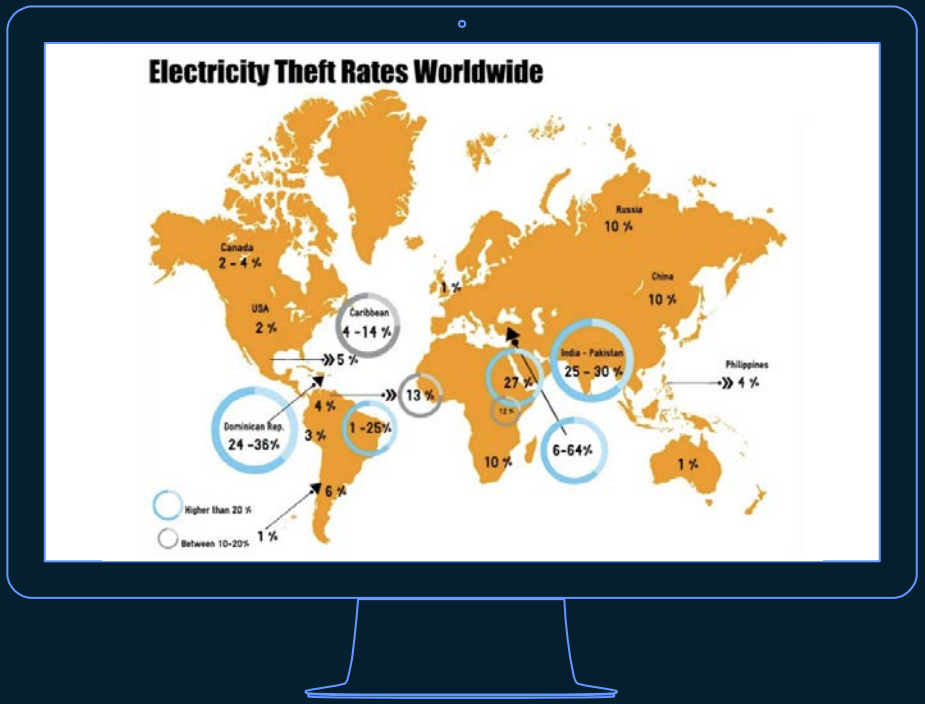
Source: *K. Shaw, Smart Meter Hardware Hacking Class, IOActive training course, IOActive Hardware Software, Wetware - Security Services, 2015.*

9. Smart Meter Data Analisis



Above: Data recorded from the considered house in 2013.
Below: Trend form house in 2013 decomposed by STL (Seasonal-trend decomposition of time series by losses) filtering method.

10. Energy theft on The World

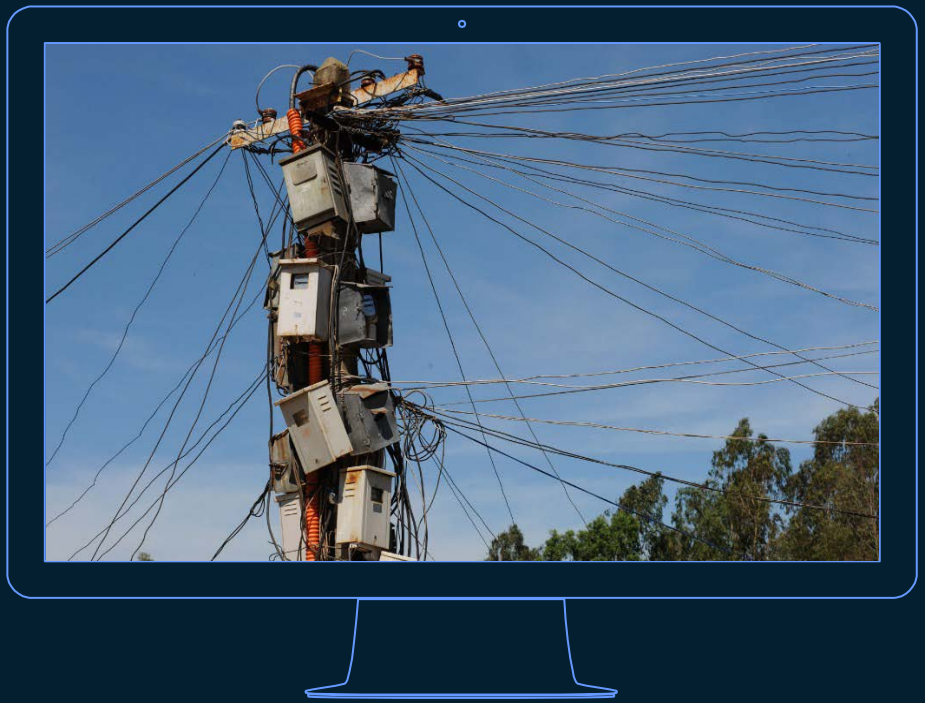


Electricity Theft Rates Worldwide 2013,
GIGAOM, Katie Fehrenbacher.

10. Energy theft on The World

Power lines in India.

10. Energy theft on The World



Prepaid Smart Meters outwit Africa's power thieves.

By Peter Shadbolt for CNN Updated 1000 GMT (1800 HKT) October 27, 2014.

Thank you for your attention

ANNA MAGDALENA KOSEK
Technical University of Denmark
Department of Electrical Engineering
Denmark, Roskilde 4000
Email: amko@elektro.dtu.dk

ROBERT CZECHOWSKI
Wroclaw University of Technology
Department of Electrical Power Engineering
Poland, Wroclaw 50-370
Email: robert.czechowski@pwr.edu.pl

CPS Week
Vienna, 11-14 April 2016

Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG2016)

This presentation (and paper) was realized within NCBR project: ERA-NET, No 1/ SMARTGRIDS/2014, acronym SALVAGE: *Cyber-Physical Security for the Low-Voltage Grids.*

Wrocław University of Technology

DTU Danmarks Tekniske Universitet