A Smart Meter and Smart House Integrated to an IdM and Key-based Scheme for Providing Integral Security for a Smart Grid ICT

Vilmar Abreu[1],Altair Santin[1], Alex Xavier[1], Alison Lando[2], Adriano Witkovski[1], Rafael Ribeiro[1], Maicon Stihler[1,3], Voldi Zambenedetti[2], Ivan Chueiri[2]

[1]Graduate Program in Computer Science / [2]Polytechnic School / Pontifical Catholic University of Parana, Curitiba - Brazil

[3]Federal Center for Technological Education of Minas Gerais, Leopoldina, Minas Gerais, Brazil

{vilmar.abreu, santin, alex.xavier, alison.luis, adriano.wit, rcr_raf}@ppgia.pucpr.br, stihler@leopoldina.cefetmg.br, {voldi.zambenedetti, i.chueiri}@pucpr.br

***Abstract**: The literature does not present integral solutions to allow using the same credential to access the smart meter and smart house from an electric utility and vice-versa. The main reason being the technology gap in the communication between the Advanced Metering Infrastructure (AMI) and the Internet. The technology used in the Internet domain to communicate with Data Concentrators (DC) and the electric utility is more powerful than the technology used in the communication between smart meters and the DC, which is bandwidth limited and better suited to the Internet of Things (IoT) domain. Therefore, we are proposing the use of Identity Management (IdM) and a key-based scheme to enable the integration of IoT and the Internet using the same credentials, without creating a security bottleneck in the communication. An additional security mechanism is provided in the smart house context to isolate the house from direct accesses from the Internet, though allowing the utility to reconfigure the electric power consumption profile to avoid a potential blackout, for instance. Our proposal includes multi-sensor anti-tampering techniques to provide physical protection to a smart meter, in conjunction with a multilevel integrity mechanism to provide logical protection to its resource-constrained microcontroller, given the smart meter is a key component to mitigate electricity consumption fraud. The prototype has shown that our proposal is feasible for protecting the smart house, smart meter and the end-to-end communication between smart meter or house and the utility.*

***Keywords**: Smart Meter Physical and Logical Security; Multilevel Integrity Protection; Tampering Detection; End-to-end Protection in Smart Grid ICT; Reconfiguration of Smart House Electric Power Consumption; IdM integrating the Internet and IoT Technologies.*

1. INTRODUCTION

In the smart grid age, it is supposed that an electric utility can interact online [1] with smart houses to access individualized (categorized) home appliances' power consumption and the smart meter to get the customer's electric power consumption [2]. Additionally, it is expected that smart meter manufacturers can access the device for maintenance purposes, including firmware updates and upgrades. Despite the advances in this area, an end-to-end secure mechanism that integrates the electric utility ICT (Information and Communication Technology) and smart meters cannot be found in the literature or in the market. The proposals in the literature partially offer security solutions, e.g., for secure communication between a smart meter (SM) and a Data Concentrator (DC) [3].

The bandwidth available to transmit data from a SM, that is also a low powered processing system, to a DC is limited [4]. This bottleneck impairs the integration of a SM with the technologies used in the communication between the DC and the electric utility, which uses an MDMS – Meter Data Management System or SCADA – Supervisory Control and Data Acquisition. The DC domain (borderline between the technology contexts of Internet and IoT – Internet of Things) usually changes the symmetric-key, used to protect the communication with the SM, to an asymmetric-key protection to communicate with the utility. Therefore, the DC may become the weakest security point, because the content is unprotected when the crypto-key system is changed. The lack of interoperability and standardization creates a technological gap that hinders the support for easy and secure technology integration between the electric utility and the SM and vice-versa [5]. This limitation leads the industry to use weak identification and authentication systems, such as hard-coded passwords – reported in Wired [6] or hard-coded crypto-keys – as reported in InfoWorld [7] and Hacker News [8] (in all cases exposing the SM to security risks). Therefore, an integral solution for securely connecting the Internet and IoT contexts is needed.

An IoT device is exposed to physical and logical threats. Tampering is the intentional physical modification of a device's functionalities, while a logical attack is the intentional software misuse to cause malfunction or to gain control of the device, aiming to compromise or corrupt the internal state of its components. In general, physical threats are any kind of device tampering and logical threats come from the communication (networking) system. Attacks of both types aim to obtain an illegal advantage.

The microcontroller (μC) is responsible for dealing with energy measurements, communication tasks, and other peripherals. It is usually embedded in a SM and has limited

resources. The security in a SM is a critical issue [9] from the electric utility's perspective because its real-time measurements can be modified through tampering or attacks to the SM's networking.

A multitasking and preemptive Real-Time Operating System (RTOS) can deal with anti-tampering mechanism requirements. However, simple μCs that equip the SM do not have enough registers to support different security modes in hardware (i.e., user and privileged modes). Therefore, the RTOS cannot implement native capabilities to deal with multilevel integrity mechanisms, as the required secure mode is unavailable in hardware.

SCADA systems enable control and data acquisition of components from various infrastructure services [10]. SCADA can facilitate the electric power load adjustment of a smart grid, requiring the reconfiguration of customers' consumption profiles to reduce the occurrence of blackouts [11].

Smart grids may use the benefits of smart house (SH) automation to possibly perform energy consumption reconfigurations. Moreover, SH enables a user to change his/her energy consumption profile to adapt to seasonal electricity rates, reducing costs. A smart house's appliances provide controllability and energy efficiency in a smart grid, enabling the interaction between the electric utility and their customers to improve decision making about energy consumption [12].

In summary, we are proposing a SM case cover with anti-tampering protection to avoid physical/internal access to the IoT device and an anti-tampering power supply mechanism to enhance the smart features of the SM, as well as a hardware-equivalent secure mode to the RTOS using MLSM (Multilevel Security Mechanism). Additionally, we are proposing the isolation of smart house from direct Internet access, preventing an attacker from remotely controlling smart meters [13] and houses, or from violating the privacy of residents by monitoring their energy consumption habits [14], [15]. We strive to provide the electric utility with a safe way for reconfiguring electric power consumption profile in smart houses (e.g., to avoid a potential blackout). Furthermore, we are proposing a symmetric crypto-key scheme associated with Identity Management (IdM) to provide end-to-end data protection, without requiring an extra effort from RTU (Remote Terminal Unit, attached to smart meter) to interact with an Internet server, unlike proposals from the literature.

The main contributions of this paper are (i) integration of a multi-sensor anti-tampering technique to enhance the tampering detection; (ii) development of a mechanism to allow SM operation with at least two electrical elements; (iii) description of a multilevel integrity mechanism to mimic the hardware privileged mode protection for a μC; (iv) isolation of the house from direct Internet access, while allowing external entities to access consumer profiles and power consumption features; and (v) description of a mechanism that uses the same security credentials to integrate the utility company to the smart meter and vice-versa.

The remainder of the paper is organized as follows: Section 2 presents the related works; Section 3 presents the physical protection of the SM; Section 4 describes the proposed SM multi-level integrity system. Section 5 presents the IdM integrating the Internet with the IoT context; Section 6 addresses Smart House integration with the utility ICT; Finally, Section 7 draws the conclusions.

2. RELATED WORKS

This section will address some literature works that present proposals using IdM for IoT/Smart Grid, Security for Smart Meters, and Smart Houses.

Liu et. al [16] designed authentication and access control methods for IoT. The authors proposed the use of OpenID and Role-based Access Control (RBAC) in the IoT context. The authors selected well-known security mechanisms, though they did not address how the integration of these robust mechanisms with *resource-constrained* devices should be performed. Additionally, message encryption and SSO are not discussed.

The work of Chin et. al [17] proposed a framework of Machine-to-Machine (M2M) authentication in smart grids. The proposal is based on digital signatures. The main problem of the proposal lies in the exchange of crypto-keys made in the data concentrator, which creates a single point of failure.

Saxena [18] proposed an integrated authentication protocol for smart grids. The proposal uses asymmetric and symmetric key cryptography to protected the communication with the electric utility. Even though the authors call it a lightweight protocol, the proposal uses hash and public key operations, which are not recommended for use in general IoT devices.

Some authors propose anti-tampering techniques to detect some specific violations of SM and to generate warnings. For instance, Mohammad et al. [19] presented an anti-tampering strategy to detect phase/neutral bypass and the opening of the case cover, but the mechanisms are standalone and can produce false positive/negative for which countermeasures are not discussed.

Tangsunantham and colleagues [20] proposed the inclusion of bypass and case cover opening anti-tampering protection in SM. However, an attacker can use phases from two separate SM, for instance, to bypass the protection without being detected, as the load in each phase is not measured individually. Kadurek and colleagues [21] proposed tampering detection by identifying large loads switching, though the proposal only identifies load variation without proposing countermeasures.

A multilevel integrity mechanism (MLSM) implemented as Low Water-Mark Mandatory Access Control [22] can provide logical security that mimics the hardware-based secure mode, called hardware-equivalent secure mode. Brasser *et al.* [23] proposed a secure inter-task communication in an RTOS to enhance the system protection, considering that an ARM processor has hardware support for memory and privileged mode protection.

In the literature, residents can interact with the house's appliances (i.e., with their embedded systems), which are accessible directly from the Internet [24], [25] and [26]. Proposals allow the reconfiguration of customized energy consumption profiles but add an additional cost to maintain the embedded systems. In addition, exposing appliances to the Internet implies risks to the security of the residents.

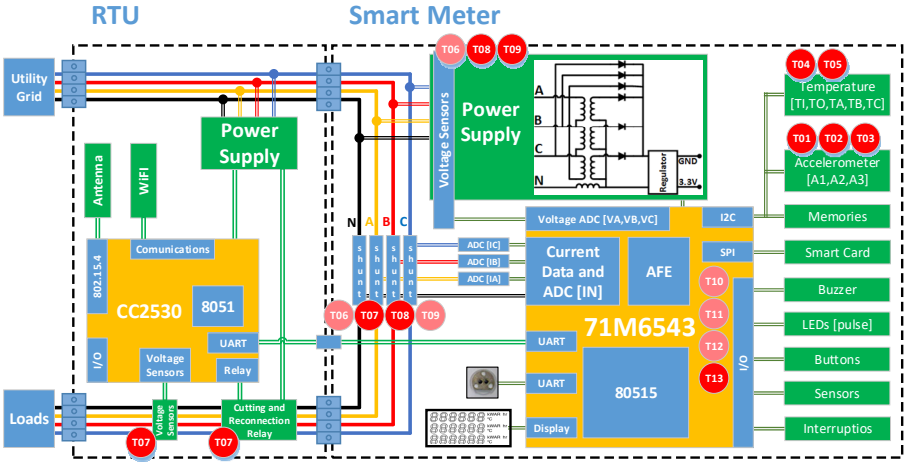

Figure 1 – IoT-Smart Meter Overview.

A vulnerability in the house appliance may be exploited to expose the resident's data or to enable an attacker to control the appliance [27]. Symantec reported 31.716 devices infected with a Linux worm named *Linux.Darlloz* for mining Mincoins, Dogecoins or Bitcoins in domestic routers, set-top boxes, security cameras, printers etc. [28]. A solution to integrate the utility's ICT and the smart house without exposing the appliances to the Internet is required.

3. SMART METER PHYSICAL SECURITY

The SM is an IoT device with three main smart features: the energy measurement, two-way communication (AMI – Advanced Metering Infrastructure) and relay for remotely cutting or reconnecting the power [29]. Examples of technologies used in the AMI or Neighborhood Area Network (NAN) are ZigBee, PLC (Power Line Carrier), and 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) [30].

The deployment of smart meters has been a strategic target for the utility companies to control energy consumption in real-time and to reduce energy theft and fraud (e.g. in Brazil, the amount of losses is about 7.5 MW per year). The utilization of the SM allows the utility to combat frauds [31], currently caused mainly by SM tampering.

The proposed IoT-SM with an anti-tampering system is presented in Figure 1. The schematic diagram is composed of two main components: the RTU and the SM. The RTU is a device directly connected to the energy grid and the SM device.

The communication interfaces are WiFi CC3000 used to connect to the smart grid and 802.15.4 CC2530 for connecting with the IoT device. The RTU has an exclusive three-phase power supply designed to supply the relay (12V) and the CC2530 board (3.3V). Moreover, it contains a sensor to detect any voltage presence when the relay is turned off; this can contribute with anti-tampering techniques. The relay is fundamental to switch the energy on or off when a tampering attempt is identified, or to respond to an electric utility request. The communication between the RTU and the SM uses an optically isolated bidirectional communication protocol.

We attached four shunt resistors (sensors) to the SM, one to the neutral and three to the phase for current measurement (Figure 1). The three phases are directly linked to the respective analog-to-digital converter (ADC) as input for the µC. The power supply contains the voltage sensors and the proposed power supply circuit. It represents the energy interface to display, optical communication for external reading (standard protocols), buttons (reset and management), and LEDs (W and V pulses). Temperature and accelerometer sensors are connected by an I2C interface to implement the anti-tampering mechanism. The buzzer is used as an alternative alarm.

The 71M6543 IC (Integrated Circuit, Figure 1) has a limited memory size (256 bytes), that are not enough to save logs or data about detailed power consumption. Therefore, the data needs to be saved in an external memory or sent to a server. We used a smartcard to ensure the protection of access and the integrity of the data, as well as other critical information such as cryptographic keys. Moreover, we used one mass memory, EEPROM, connected via SPI interface to 71M6543 and is used to record tampering attempts and the history of energy measurements when communication is unavailable (i.e., for backup purposes).

3.1 Tampering and Anti-tampering

In Table 1 we describe all tampering techniques present in the literature, and relate them with the sensors identified as T01 - T13 in Figure 1.

TABLE 1 - Tampering and Anti-tampering techniques.

Tampering	Description	Anti-tampering (Literature)
T01: Anomalous vibration of the electric SM's case cover	Indicates the SM is under a physical intrusion attempt (e.g. using a drilling machine).	Unknown.
T02: SM board violation	Indicates the SM is risking physical damage/attack or beating.	Unknown.
T03: Electric SM case cover violation	Indicates the SM is exposed.	A switch is proposed in [19] and a Light Dependent Resistor is proposed in [20] to identify the opening of the electric meter case cover.
T04: SM components	Overheating the SM trying to burn or melt internal components	Unknown.

burning by overheating	(such as a transformer), hoping to disable specific functionalities.	
T05: High voltage or electromagnetic pulse to burn a circuit	Attempt to burn sensors by applying a high voltage pulse directly on the sensor to disable the SM's measurement capability.	Unknown.
T06: Cogeneration subvention by inversion of quadrants	Attempt to use a power cable coming from the grid as cogeneration energy input to subvert the cogeneration energy measurement.	Unknown.
T07: Phase Bypass	Bypass one, two or three phase elements, maintaining the neutral connected to the grid.	Measure the neutral current and comparing it with the sum of the other three elements, phase A, B and C [20].
T08: Neutral line disconnection	Disconnection of the neutral reference to destabilize the SM's measuring system.	Measure the current on the neutral and the phases. The tampering is identified when there is current in the phases and there is no current in the neutral [19].
T09: SM bypass by removing the measuring loads	Connecting some load closer to the SM, aiming to bypass the phases and the neutral.	Measurement of the abrupt voltage variation by the SM when illegal load is triggered [16] [19].
T10: Illegal load in a local area	Adding load in the grid randomly between the SMs in a way that is not perceived by them (e.g. machine that demands high power).	A centralized SM is added in a local area of the grid as a master for a cluster of SMs. The sum of energy consumption reported by all SMs in such a cluster must be equivalent to the measurement from the centralized SM [19].
T11: Illegal load with appliances' loads identification	Adding load randomly in the grid in a way that is not perceived by the closest SM (e.g. appliance with very low power consumption).	Use machine learning techniques to identify pre-standardized load patterns and compare it with those identified by the system [32].
T12: Frequency of connections and disconnections	A high number of connections and disconnections of the wire phase, indicating some external control to hide an electricity theft.	Unknown.
T13: Battery damage or removal	Damage or disconnection of the battery to avoid tampering detection, attempted when the electricity is off.	Unknown.

Our proposal brings enhancements in the anti-tampering mechanisms that can be summarized as shown in the following.

- T01, T02 and T03: Implementation of three accelerometers sensors, one on the board and two on the SM's electrical case cover, allowing the identification of drill machine vibrations, strokes, and case opening attempts.
- T04: Implementation of temperature sensor inside and outside the case cover that can identify an unusual heating that can characterize an element-burning attempt, when compared to historical average records.
- T05: Implementation of a temperature sensor on the current sensors that can measure temperature spikes that can indicate an overvoltage, attempting to damage some internal components (not the entire SM).
- T07: Measurement of the neutral current compared with the sum of the other three elements, phases A, B and C. If the sum does not match, the relay is turned off and the load voltage is tested. If the test results in an incompatible voltage on the load side, a tampering is happening.
- T08: The proposed power supply creates a virtual neutral reference, ensuring the SM works with or without battery, given that it has at least two elements connected between the three phases and the neutral.
- T13: RTC (Real Time Clock) is evaluated, when the null value is identified the battery may be off or some reboot condition was activated while trying to make illegal changes while the SM was powered off.

On the sections 3.2 and 3.3, we focus in the more relevant aspects of our proposal for anti-tampering techniques, using the three accelerometers and a power supply with a virtual neutral.

3.2 Anti-Tampering Mechanism based on a Power Supply

The voltage supply is designed to operate at least with two grid elements connected between phases A, B, C or neutral. A virtual neutral reference is automatically generated when the neutral element is disconnected from the electric utility. This is important to prevent a T08 attempt (section 3.1). It is important to highlight that using a simple circuit based only on diodes to rectify the sinusoidal wave from the grid, it necessarily requires the presence of the grid's neutral as a reference for it to work correctly. We decided to add a circuit based on voltage transformers in our proposal to obtain the virtual neutral element.

3.3 Detecting SM Case Intrusion

The anti-tampering techniques proposed in [19] and [20] are prone to raising false alarms. This might happen when a vibration is provoked by a bus crossing the street or a more sophisticated technique is applied, like a machine drill being used to damage or interfere with a specific SM component (e.g. regulator, accelerometer, memories, or battery). Our proposal applies three accelerometers to avoid these tampering (T01, T02 and T03) attempts, one attached to the SM's board and two attached to the inside side of electric SM's case cover.

Opening the electric SM cover can be observing the angle measured between the axes (X, Y, Z) of the accelerometers, given that during an intrusion, the board's accelerometer tends to stay undisturbed while the other two show an important angular variation relative to their initial position. Damage attempts caused by beating on the SM's case can be registered by abrupt and strong angular variations, read in the three accelerometers. A drill applied to the SM's cover can be detected by a subtle angular variation measured by the accelerometers, observing the drill pattern in different parts of the case cover surface.

3.4 SM Implementation

The microcontroller (μC) chosen for the SM was the integrated circuit (IC) *71M6543* by Maxim (datasheets. maximintegrated.com/en/ds/71M6543F-71M6543H.pdf). This IC is based on the Intel 8051. One of its highlights is the

presence of an independent 32-Bit computing engine that can calculate the voltage and current provided by a 22-bit delta-sigma ADC (analog to digital converter), meeting the requirements of ANSI and IEC with 0.1% accuracy over a 2000:1 current range.

The set of resources for voltage and current acquisition and processing is called Analog Front-End (AFE). The AFE is useful because it removes the complexity and processing load of RMS voltage calculations in a 8051-based IC. Development in an architecture that is a *de facto* standard brings the benefit of portability, it can be migrated with minimum effort to other Intel 8051-based architectures. Thus, the solution can be ported to other SMs or IoT devices with similar features.

Comparing the sum of the currents (provided by AFE) on the three phases and the neutral current allows the detection of T07 and T08 tampers (section 3.1). The SM can register the occurrence of tamper when the neutral current does not match the current in the phase, considering the known energy losses in the transmission line (neutral and phases' wires). The occurrences are always logged because the tamper can be attempted many times in a given period. The tamper techniques T01, T02 and T03 are detected by reading the values of axes (X, Y and Z) of each accelerometer and computing the differences.

The tamper techniques T12 and T13, always check the SM's initialization. Each time the SM is started, the event's time is recorded. When the restart interval is too short, it indicates a T12 tampering. SM restarts with a good battery condition and the RTC reset indicates the battery was deliberately removed while the SM was powered off, pointing to T13.

The physical attack techniques considered in this paper were classified into two categories: warning and critical. The warning category is designed to identify techniques that affect only the electricity measurement (T06, T07, T08, T09, T10 and T11). The critical category corresponds to attacks that target directly the SM (T01, T02, T03, T04, T05, T12 and T13).

After the SM setup, we focus on the evaluation of the physical protection because it is easier to evaluate. One grid line was drawn along the electric SM's case cover surface. Afterward, we used a drill machine to drill each crisscrossed grid line to learn how the drill vibration pattern can be identified as a tampering attempt T01. T03 was tested by recording the difference between the three axes, measured in the accelerometers, when the sensor on the board records a small perturbation while the other two sensors detect a strong variation on the axes. T02 was tested by hitting the SM case and observing the oscillation registered by the three sensors simultaneously.

The accelerometer observed the more intense vibration closer to the drill and the vibration intensity decreased as the drill was moved away (T01). The SM's cover opening presented a large variation in the axes recorded by the accelerometers closer to the cover's edge, because they are turned around first (T01). Pulling the cover generates a movement detected on all the cover's accelerometers, while the values in the axes stay unchangeable in the board's accelerometer (T03). Hitting the case cover creates a large vibration spike in a very short time interval, identified by all accelerometers except the one on the board (T02).

The proposed power supply (T08) was tested by connecting the four elements from the grid (phase A, B, C and neutral) to the SM and disconnecting them in sequential order until the combination that maintains the power supply output in 3.3V was identified. The results showed that if two or more elements are connected to the grid, the power supply output remains in 3.3V, thus making it possible for the SM to work without a neutral connected to the grid. Moreover, even when a half-phase (split phase) condition (partial power outage) is identified, caused by a grid failure or tampering attempt (connecting two half-phases is equivalent to one full phase), the power supply still works and the tampering can be identified. The minimal voltage, in half-phase, is about 60VAC (~80VDC) that remains above the minimal input voltage (70VDC) to keep the regulator in operation. Even when the minimal voltage cannot be reached, the SM continues to work with power supplied by the battery.

4. SMART METER LOGICAL SECURITY

The 8051-based μC presented in the proposed SM does not have hardware-level features to support secure mode, as said before. Therefore, we are porting an RTOS code to a SM based on an 8051 μC and adapting it to support an MLSM (Multi-Level Security Mechanism). The MLSM embeds a multilevel integrity mechanism based on the BIBA model [33], aiming to provide the hardware-equivalent secure mode in software-level, supported by the RTOS.

The LoMAC [22] is a BIBA model implementation where the subjects and objects are labelled with low or high integrity. A high integrity object intends to maintain the data integrity by allowing content modification (write) only by high integrity subjects. However, high and low integrity subjects can change (write) on low integrity objects. Subjects with high or low integrity can read any object labelled as high integrity. A low integrity object, on the other hand, can be read only by low integrity subjects, intending to avoid tainting the high integrity subjects. We adopted the LoMAC integrity approach in our proposal.

Beyond providing the hardware-equivalent secure modes, the MLSM intends to protect the memory space configuration of the AFE, to safely store the calibration data, consolidated voltage, and current energy measurement. The objects (tasks and resources) and subjects are stored in the flash (read-only) memory. We labelled the subjects and objects as being high or low integrity.

Multilevel integrity subjects are the *administrator* (high integrity) and the *operator* (low integrity). Multilevel integrity objects are (i) tasks (high integrity): *Idle*, *InterfaceSmartCard* and *InterfaceUser*, and (low integrity): *InterfaceSerial* and *CheckTemperature*, and (ii) resources (high integrity): *Clock System*, *Calibration Temperature* and *Smart Meter Calibration* and the (low integrity) resource is *Output Display*.

It is possible to illustrate the benefits of MLSM (inherited from the BIBA model) with a networking example. Every packet coming from the network is considered as a low integrity object. Assume that someone discovered the administrator

password and tried to authenticate herself into the SM from the network. The login will happen successfully, but the administrator session will be executed in user mode (low integrity) because the network access itself has low integrity.

A similar situation can happen after a critical tamper, in this case the MLSM lowers the integrity level of all objects and subjects as a countermeasure. Therefore, the risk of a physical or logical attack damaging the SM is mitigated.

RTOS are focused on response time and can be classified as cooperative or preemptive. In cooperative systems, a task is initiated only when the system is idle, while preemptive systems can interrupt a running task can at any time to handle real-time events. Thus, if an intruder attempts to tamper with the SM, a hardware interruption catches the 8051 µC attention and this event is immediately handled to apply the corresponding countermeasures.

The SM was designed to have two states: normal and critical. The SM operates in normal state when no tampering is detected. The critical state depends on the type of tampering (warning or critical): warning may indicate a tampering attempt was detected, while critical type indicates that the system is compromised and cannot be considered as reliable anymore. The default procedure under critical state is to store the current registers' contents in the smartcard and to enable verbose logging to the remote server and/or to EEPROM. However, the power utility can define a custom contingency plan that must be previously stored in the flash memory.

Figure 2 show an overview of the logical security proposal. Event i verifies if the RTC is equal to zero and if the first boot is taking place. Next, it verifies if there was a recent boot (e.g., in less than 15 seconds earlier). The MLSM enables the verbose logging and changes the system state to critical if any inconsistency is found in these verifications, and tampering T12 or T13 is happening. The sensors are calibrated after the initial system integrity check (event ii). Afterward, the system waits for hardware interruptions (event iii), and when it occurs (event iv), the task scheduler invokes the multilevel integrity check (event v). The task integrity level (stored in flash memory) is evaluated against the subject integrity level (also stored in flash memory), following the rules of MLSM/LoMAC policy evaluation. Verbose logging is enabled and the task is rescheduled to treat an access error if the access is denied, otherwise, the task will be run in the µC CPU (event vi).

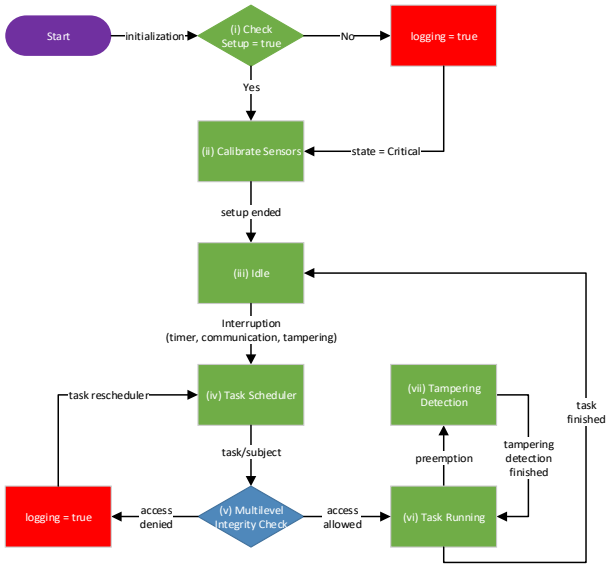

Figure 2 - Logical Security Overview.

The main hardware interruptions are (i) timer: triggered when it is time to consolidate consumption data, (ii) communication: triggered when the power utility requests data or remote access to the SM, following the key-based authentication method proposed in [34] and (iii) tampering: triggered when a tampering attempt is detected. The tampering detection interruptions are preemptive (event vii) and suspends any running task, except the multilevel integrity check engine.

4.1 MLSM Implementation

The MLSM development involved the porting of FreeRTOS 8051 specific code to an 80515 µC (embed in 71M6543 IC). The Task Control Block (TCB) of the FreeRTOS was modified to check the integrity of subjects and objects before scheduling tasks. The Algorithm 1 presents the function to write the contents of the buffer variable in the XRAM (AFE) memory in the 71M6543 (Figure 1). When requesting access to write in an XRAM memory, this operation succeeds only if the task's (subject) integrity level is higher or equal to the requested memory address (object) and the buffer size does not cause an address violation (Algorithm 1, row 3 and 4).

Algorithm 1 Verify task integrity

```
1:  function SetMemory(memoryAddress, buffer, bufferSize)
2:      if current task is low integrity then                ▷ the task is the subject
3:          if memoryAddress is high integrity then          ▷ memoryAddress is the object
4:              return Error - access denied
5:          else if memoryAddress + bufferSize causes address violation then
6:              return Error - address violation
7:          end if
8:      end if
9:      Write buffer to memoryAddress
10:     return Success
11: end function
```

The program code that writes to flash memory ensures that the FreeRTOS's integrity level is not changed in an eventual MLSM intrusion. The smartcard is used to record critical events because it provides a secure interface for storing timestamps, and to dump µC internal registers' contents and memory when the system reaches a critical state. The smartcard is also used to store a copy of the secret key provided by the smart meter manufacturer. The secret key is linked to the SM's serial number, and it is stored in the customer database of the electric utility (Figure 3).

4.2 MLSM Evaluation

The evaluation was performed using the uCsim microcontroller simulator, version 0.5.4 [35] to allow the control of the experiment's measurements. Tests were performed to measure the latency time for a task to be initialized when the system (scheduler) works exclusively in cooperative mode and in preemptive mode - task interruption occurs (tamper events). In cooperative mode, the time to begin a task, in the worst case, is the quantum time (defined by the FreeRTOS's scheduling policy) multiplied by the ready tasks queue length. In our experiments, we ran a scenario with 10 ready tasks, and the task started at approximately 847015 clock cycles, while the

task that initiated through the interruption started at approximately 345840 clock cycles. This setup time for the tampering routine to start running represents a performance gain of 250% in the preemptive mode. This approach is essential for handling tampering events that begin and end in a few milliseconds.

For the reading and writing in protected memory space tests, two tasks were implemented: *InterfaceSerial* (low integrity) e *ClockSystem* (high integrity). We measured the runtime with MLSM enabled and disabled, in order to analyze performance. The time to run the same task with memory access protection was 4.24 times greater than without it. The increase in the processing time occurred due to the integrity level validation in the subject and object, and the address violation verification (Algorithm 1, row 5).

We tested the MLSM verification (Figure 2, event v) performance. When the MLSM mechanism denies the access and enables the verbose logging, the function is performed in 2080620 clock cycles. The function is performed in 2141928 clock cycles when the mechanism allows the access, this execution time was higher due to the writing memory.

Despite the reduction in performance, the use of memory protection has the advantage of maintaining the integrity of the system data and avoiding buffer overflow attacks, for instance. The microcontroller does not have such hardware protection mechanisms. The data integrity protection ensures that calibration information and measurement data are protected even if a system vulnerability occurs.

5. IdM FOR INTEGRATING INTERNET AND IoT CONTEXT

5.1 Proposal

The SM is frequently queried to send power consumption information to the electric utility (through the SCADA/MDMS). MDMS, SCADA, AMI and SM are examples of smart grid ICT [36]. In addition, the SM can communicate with the Smart Meter Manufacturer (SMManufactory) to perform firmware updates, and to calibrate or adjust a specific hardware parameters. In any case, it is essential that the SM has a secure communication with external entities.

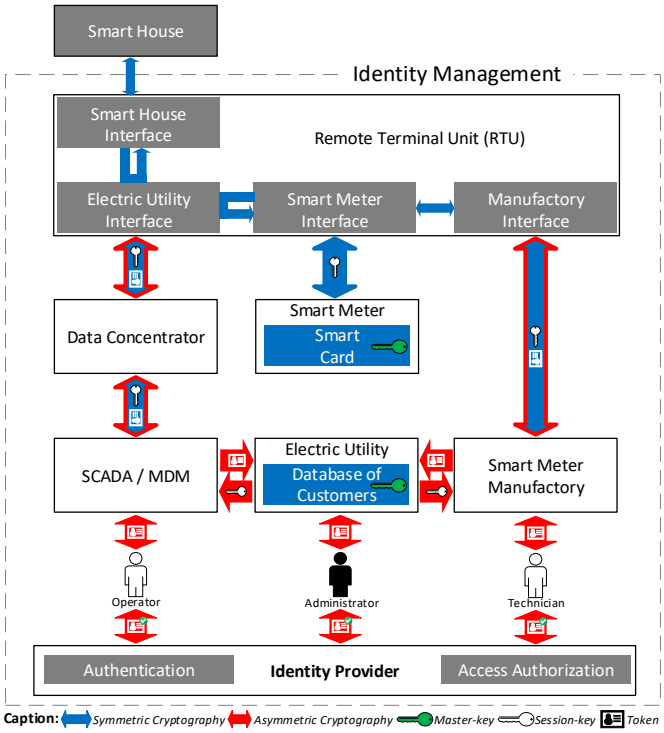

Figure 3 - Overview of IdM and Key-based integral security for smart grid ICT.

Because of the inherent limitations of IoT devices [37], the SM has limited computing resources that restrict the use of traditional communication and security protocols. Natively, an SM cannot use an encryption scheme based on asymmetric keys. Thus, the industry solution uses weak identification and authentication systems, such as hard-code passwords – reported in Wired [6] or hard-coded crypto-keys – as reported in InfoWorld [7] and Hacker News [8] (in all cases exposing the SM to security risks).

Figure 3 presents an overview of our security solution for accessing the SM through traditional systems of electric utility (SCADA/MDMS) and SMManufactory. The proposal is based on the integration of an IdM mechanism that is suitable for IoT technologies. The mechanism allows an operator to perform

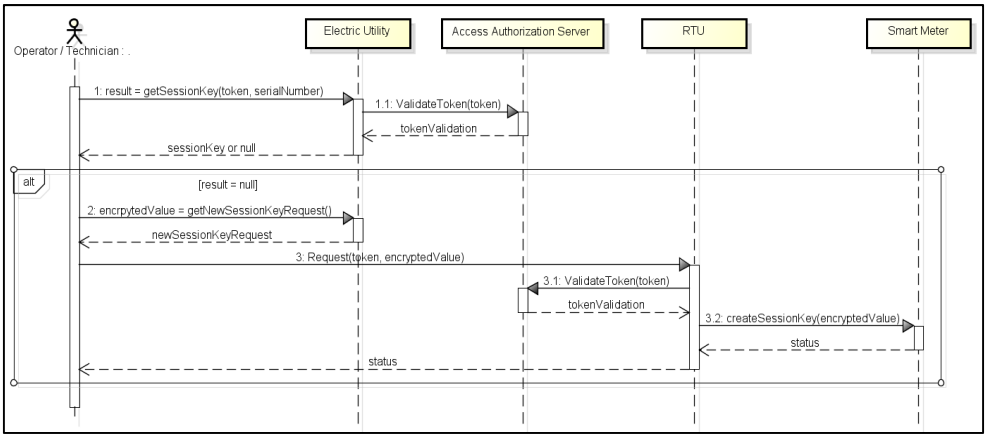

Figure 4 - Smart Meter session key call back request.

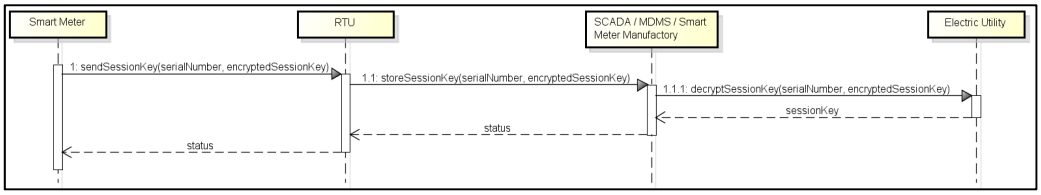

Figure 5 - Smart Meter session key generation.

authentication on SCADA/MDMS and to carry its credentials to the SM. We use the standardized cryptographic key scheme based on ANSI X.9.17 [38] to maintain the link between the authentication on SCADA/MDMS and the IoT device (SM).

Our proposal consists of the following main entities (Figure 3). The smart house contains the RTU and the SM, both IoT devices discussed in section 3 and 4. The electric utility is outside the SH (Smart House) context, it is the element responsible for mediating the SCADA/MDMS and SMManufactory access to the SM. The users responsible for using SCADA/MDMS are called an Operators, and those who access the SMManufactory are called Technicians.

We consider that the access level for a technician and an operator should be different, when she is properly authenticated and authorized and is accessing the SM. An operator can only perform the operations related to the business of the electric utility (e.g. reading energy consumption, costumer's information, fraud detection). On the other hand, the technician can only access the SM manufactory part.

Our security proposal considers the limited resources of the IoT devices (SM/RTU). Thus, we considered the SM and the electric utility to have a secret (symmetric) key, which is called the master key. The master key is stored in a smartcard on the SM and is replaced only if compromised.

The electric utility (Figure 3) is responsible for mediating operator/technician access to the SM, i.e., it is responsible for storing the master and session keys. When an operator/technician wants to access the SM, the electric utility provides the session key (if it is still valid) or requests the creation of a new one. For the operator/technician to obtain the session key, they must authenticate themselves in an Identity Provider (IdP) through the Authentication Server (Figure 3), allowing them to obtain an access token in the Access Authorization Server. The access token is an authorization granted by the resource's owner that allows an operator/technician to get the session key in the electric utility (Figure 3 and Figure 4).

If the operator/technician is authenticated in an IdP and has obtained the access token, she can request the session key to the electric utility, informing the access token and the SM's serial number (Figure 4, event 1) [34]. The electric utility validates the access token in the Access Authorization Server (Figure 4, event 1.1). If the access token validation is successful, the electric utility verifies the session key's lifetime, if it is not expired, it is returned to the operator/technician. Note that the electric utility can set policies to define when a session key expires, e.g. default lifetime of session key equal to 8 hours.

If the session key is invalid, the operator/technician must request to the SM the generation of a new session key. To perform this procedure, the operator/technician makes a request to the electric utility to create the request for a new session key (Figure 4, event 2). The electric utility builds the encrypted request using the latest valid session key and returns it to the operator/technician. This encrypted request contains information related to the operator/technician and the contents can only be decrypted by the SM.

The operator/technician forwards the request to the RTU, informing the access token and the encrypted value (Figure 4, event 3). The RTU validates the access token (Figure 4, event 3.1). If the access token validation is successful, the RTU forwards the encrypted value to the SM, and requests the creation of a new session key (Figure 4, event 3.2).

The session key generation and distribution is represented in Figure 5. Initially, the SM generates the session key and encrypts it using the master key. The key is sent to the RTU (Figure 5, event 1) with the serial number (decrypted) and the session key (encrypted). The RTU requests the session key storage (Figure 5, event 1.1) to the entity who wants to access the SM (SCADA/MDMS or Smart Meter Manufactory). As the entity, does not have the master key to decrypt the session key, it is necessary to forward the encrypted content to the electric utility (Figure 5, event 1.1.1). The electric utility stores the decrypted session key, binding it to the serial number and returning the decrypted session key to the operator/technician.

The decrypted session key allows the operator/technician to interact with the SM. The technician encrypts the content to be sent to the SM with the session key and forwards to RTU,

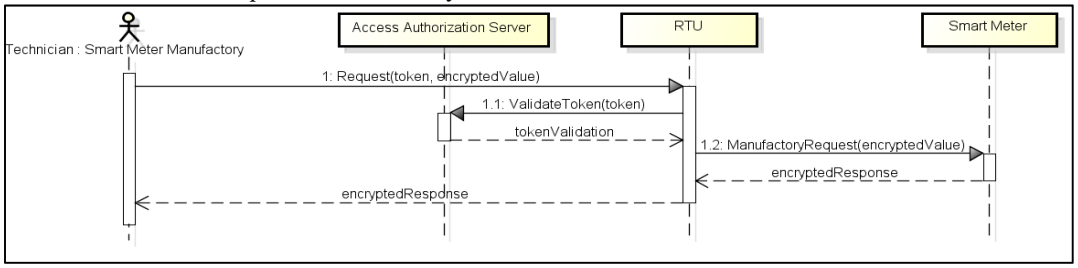

Figure 6 - Technician request to SM.

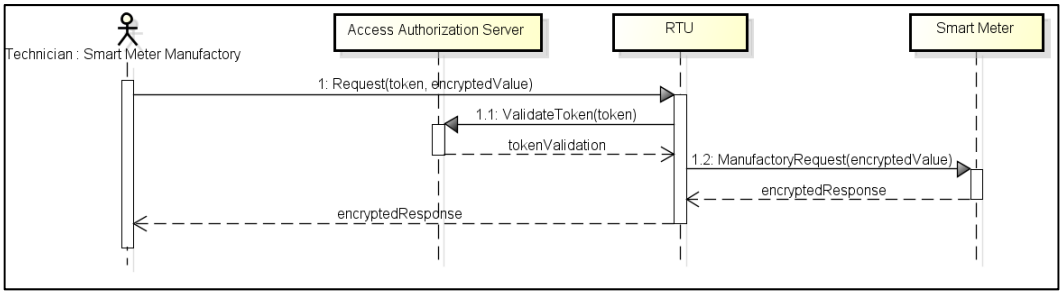

Figure 7 - Technician request to SM.

informing the access token and the encrypted value (Figure 6, event 1), to access the SM. The RTU validates the access token (Figure 6, event 1.1). If the access token validation is successful, the RTU forwards the encrypted request to the SM (Figure 6, event 1. 2). The SM decrypts the request, processes it and returns the encrypted response to the RTU for delivery to the technician.

The operator does not access the SM directly, because the operations could allow injections or other kinds of attacks aiming to gain control of the SM. We avoid session establishment by using the request queue to communicate with the SM, therefore, if an exploit is launched against the SM without a session, the malware/shellcode does not have a client and will not be as dangerous as in an interactive session.

The operator that wants to access the SM, must encrypt the contents to be sent with the session key and forward the result to the RTU, informing the access token (Figure 7, event 1). The RTU validates the access token (Figure 7, event 1.1). If the access token validation is successful, the RTU appends the request to the internal message queue and returns the request's index. The SM, at a frequency preset by the electric utility, queries the RTU any request new (Figure 7, event 2). The SM decrypts the request, processes it, and adds the response to the RTU (Figure 7, event 3). The operator queries if the request has been answered (Figure 7, event 4) and this process is repeated each time it is need.

5.1 Proposal Implementation

We used the framework Vaadin [39], JAX-RS API [40], Californium library [41], ContikiOS [42], OpenID Connect specification and Nimbus [43] to implement the architecture of Figure 3. We also used Nessus on kali (www.tenable.com/blog/installing-and-using-nessus-on-kali-linux) to test the security of the environment, and with OWASP Zed (www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project) to scan for well-known web vulnerabilities.

5.2 Security Evaluation

Our proposal implements a secret key-based scheme to provide integral security in smart grids, allowing an operator/technician to transport a credential from an Identity Provider (web) to the SM (IoT). This approach is suitable to the IoT devices' capabilities and keeps the end-to-end confidentially of a message's contents. Moreover, by using a secret-key based SSO, the proposal allows the traceability of the user's access, because they use the same session-key to access several devices.

The proposal uses a combination of security mechanisms to ensure that the security of the entire smart grid system is not compromised even when a system component (entity) is compromised. This emphasis on providing integral security is not found in the literature neither in commercial products.

In addition to the mentioned qualitative enhancement, we considered scenarios where elements of architecture are compromised in the evaluation of our proposal. In this scenario, we exploited the CVE-2016-0714 vulnerability present in Tomcat 8.0 and earlier versions. This vulnerability is related to the execution of arbitrary code in a privileged context via a web application. Table 2 shows the possible impacts for each system component when the vulnerability is identified.

TABLE 2 – Security Evaluation

Compromised component	Impact
Authentication Server	The attacker can access the home page of the SCADA, Electric Utility and Smart Meter Manufacturer, but she is not able to perform any operation because she does not have the access token.
Access Authorization Server	The attacker cannot access the Server, because the Identity Token must have the user authentication information. This identity token is validated online in the Authentication Server.
Electric Utility	The attacker has access to the smart meter's master keys, but she is not able to access the smart meter (through the RTU) because she does not have the access token.
Smart Meter Manufactory / SCADA / MDMS	The attacker cannot access the Electric Utility because she does not have the access token. The attacker is not able to access the smart meter (through the RTU) because she does not have the access token neither the session key.
Data Concentrator	The attacker cannot access the confidential message's content because it is encrypted using the session key.
Electric Utility Interface	The attacker cannot access the confidential message's content because it is encrypted using the session key. The attacker cannot inject/access the smart meter because she does not have direct access to the Smart Meter Interface.
Manufactory Interface / Smart Meter Interface	The attacker cannot access the confidential message's content because it is encrypted using the session key.
Smart Meter	The smart meter has physical and logical protection. Therefore, we hope she will not be able to control the SM because logical protection avoids attacks coming from the communication interface and physical protection avoids physical tampering.

As a security evolution conclusion, until now, we could not identify vulnerabilities in our proposed mechanisms.

5.3 Usability Evaluation

The goal of this test was to show the enhancement in the usability of the proposal. Figure 8 shows the comparison

between the number of messages exchange required for an Operator/Technician to communicate with an SM. We considered 4 scenarios: (i) "SSO + current Session-key" representing the scenario described in the proposal, when the Operator/Technician already has a session key; (ii) "SSO + new Session-key" representing the scenario described in the proposal when the Operator/Technician does not have a session key (Figure 4 and Figure 5); (iii) "Auth + current Session-key" representing a scenario where the Operator/Technical credentials are not ported to the SM, thus, requiring to perform a single authentication for each SM that she wishes to access, however, the operator already has the SM session key; (iv) "Auth + new Session-key" representing the scenario described in item 3 without the session key, thus following the procedures defined in (Figure 4 and Figure 5).

When a session key needs to be generated, due to a first access or a lifetime expiration (Figure 4, event 2), the SM must be requested to generate a new session key following the procedures defined in Figure 6 (Technician) or Figure 7 (Operator). Thus, the SM initializes the procedure defined in Figure 5. This procedure implies the addition of 13 messages to the Operator procedure and 10 messages to the Technician procedure. The Operator has a higher increase because SCADA/MDMS does not directly access the RTU, unlike Smart Meter Manufactory.

It is possible to observe that the generation of a new session key increases the number of messages over the network, as well as requiring the SM (low power processing device) to process a new symmetric key (128/256 bits). However, the advantage of using a new session key is to reduce the risk of key discovery through cryptanalysis. The lifetime of the session key can be parameterized by the electric utility, aiming at balancing security and performance.

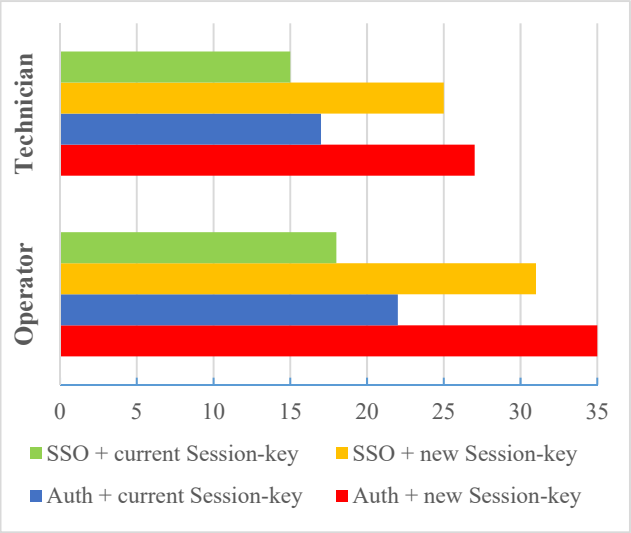

Figure 8 – Comparison between Auth/SSO approaches.

The use of SSO and Session-key reduces the number of messages exchanged, which provides usability improvements. The RTU requests authentication of the Technician/Operator (Figure 6 and Figure 7, event 1.1) after the validation of the access token in the absence of a SSO mechanism. This implies the addition of 2 and 4 messages respectively. Figure 8 shows the advantage of its usage to access one SM, though usually a technician/operator accesses many SMs in a day. Therefore, the usability enhancements will be multiplied by the number of SM accesses at end of the day. However, it can be noted that the benefits of using SSO and session-keys are primarily related to security and qualitative improvements.

6. SMART HOUSE AND UTILITY ICT

The proposal implements a Smart House (SH) accessed through a smart house interface (RTU component, Figure 3) and considers a scenario of energy consumption management and operation. The aim is to deal with the requirements of the electric utility and the residents' demands, without exposing the house appliances to the Internet [44].

The proposal involves three main components (Figure 3): electric utility interface, smart house interface, and a mobile phone. To maintain the isolation and integrity of SH, electric utility interface and smart house interface are services running on RTU. Electric utility interface enables the communication between SCADA/MDMS and the SM, maintaining a request queue, i.e., a request from the electric utility to reduce the consumption.

The electric utility can inform SH about seasonal changes in the electricity rates that will affect scheduled appliances, thus avoiding spending unnecessary money when a task could be rescheduled to a period with lower cost rates. Smart house interface is accessible only in the HAN (Home Area Network), being responsible for storing residents' mobiles admission information and consumption profiles (that includes desirable seasonal electricity rates for each appliance). This interface reconfigures the consumption based on the profiles (when the mobile is not reachable from RTU due to weak signal).

We use two distinct services (electric utility interface and smart house interface) to mitigate attacks from the Internet. SCADA/MDMS can only send requests to the electric utility interface. Periodically, smart house interface reads the electric utility interface request queue. There is no direct access from the Internet to the SH. However, the utility can still interfere with the SH consumption setting, by invoking one of different consumption profiles. Pre-registered mobiles create and update SH consumption profiles [44], [45].

Consumption profiles can be created by combining appliances consumption patterns and residents' needs. For instance, we present two profiles that classify appliances as essential (e.g. refrigerator, freezer) or desirable (e.g. laundry machine, stove, microwave) [44]. This classification will be used in the process of energy consumption reduction accessed by utility. Our proposal assumes that the utility has a system (e.g. SCADA/MDMS) integrated with SH that can obtain consolidated energy consumption from each SM. Thus, by monitoring electric power supply and demand, in a city or village, is possible to predict a blackout, for instance.

If a blackout cannot be detected in advance to activate a spare electric power generation system, or such a system is expensive to be maintained, our proposal is suitable to help.

Based on the consumption monitoring it is possible to identify critical situation for power supply and enable SCADA/MDMS to require users (smart house interface) to change their consumption profile, meaning that an essential profile can be active to avoid a blackout [44]. Thus, it is possible to mitigate a blackout because SH has an online integration with the electric utility ICT. Moreover, it is possible to deploy other facilities, e.g. complex fraud detection (that is detectable considering only the SM), power quality and health system monitoring.

6.1 Smart House Implementation

The SH was integrated into the implementation of the architecture of Figure 3, described in section 4.2. The smart house interface was implemented using JAX-RS API [40], in this case, we used metasploit on kali (www.metasploit.com) to test the security of environment [44].

7. CONCLUSION

This work presented an integral solution for secure communication between SM or SH and the utility ICT. The integral security was addressed in order to overcome the limits of AMI communication. In addition to secure communication integration, it also enabled the usage of the same credential in different technological contexts, such as the Internet and the IoT. Our proposal applies an approach that avoids hardcoded passwords or crypto-keys, which are limitations present in the literature and market solutions, to allow access from the Internet to IoT devices and vice-versa, despite the intrinsic technological limitations of each scenario.

Smart house responds to electric utility requests through an SH service that intermediates communication. Thus, when the utility needs to reduce energy consumption, e.g. to avoid a possible blackout, it communicates with a service that exclusively receives external requests (electric utility interface). For security reasons, it is necessary that another service (smart house interface) detects the utility requests to start a process of energy consumption reduction in a smart house (this process runs automatically). A similar procedure is executed when a seasonal electricity rate is changed. Therefore, the SH is accessible, though not directly accessed from the Internet, thus avoiding possible security attacks.

The link between the AMI and the Internet, provided by DC, protects the message in an end-to-end fashion operator/technician an SM. The DC cannot access message contents, it encrypts the context with symmetric session-key – suitable for IoT, or asymmetric keys – suitable for the Internet. An additional security feature is provided by the IdM to protect the DC, the authorization token. Only a user authenticated in the IdP can obtain such a token, therefore the DC is protected against denial of service attacks, for instance.

Physical and logic protection applied to the SM is a requirement of almost every IoT device that is physically accessible by anyone, and logically susceptible to attacks that come from the communication (network) interface. We integrated a multi-sensor anti-tampering technique aiming to enhance the tampering detection solutions, and to decrease the false positives/negatives. Moreover, unlike the literature, we use accelerometers in the electric SM's case cover to avoid false positives. We also developed a novel three-phase power supply with a virtual-neutral, allowing the SM to operate with at least two elements out of four (three phases and one neutral), including two half-phases (split phase).

We provided the SM with a novel logical protection on the RTOS, given 8051-based μC do not have the hardware support to implement secure mode. The MLSM also protects the internal resources of the μC and can be an important strategy, used as a countermeasure when tampering is detected. Finally, as the SM's firmware is stored in a flash memory, the program, subjects and objects are not prone to modification in case of malicious intrusion on the MLSM.

As a future work, we expect to deploy our proposal in our partner, Copel (electric utility), in order to analyze the benefits of our proposal in a real environment.

ACKNOWLEDGEMENTS

This work was partially sponsored by the Brazilian National Council for Scientific and Technological Development (CNPq), grants 307346/2015-3 and 404963/2013-7. Vilmar Abreu Junior wishes to thanks to CNPq for scholarship granting, process 381612/2014-7. We wish to thank for the valuable contribution to the electric engineering Alison Lando, Ivan Chueiri, Voldi Zambenedetti and Marcio Hamerschmidt (Copel). Moreover, we thanks to our partners from industry, Siemens and Copel.

REFERENCES

[1] Z. Cai, M. Yu, M. Steurer, H. Li, Y. Dong. “A network model for the real-time communications of a smart grid prototype,” in Journal of Network and Computer Applications, vol. 59, pp. 264-273, 2016.

[2] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, “A Survey on smart grid potential applications and communication requirements,” in IEEE Trans. Ind. Informatics, vol. 9, no. 1, pp. 28–42, 2013.

[3] T. Shiobara, P. Palensky, and H. Nishi, “Effective Metering Data Aggregation for Smart Grid Communication Infrastructure,” Proc. of IECON, pp. 2136–2141, 2015.

[4] M. Emmanuel, R. Rayudu. “Communication technologies for smart grid applications: A survey,” in Journal of Network and Computer Applications, Volume 74, pp. 133-148, 2016.

[5] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, K. Wasielewska, “Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective,” in Journal of Network and Computer Applications, , vol. 81, pp. 111-124, 2016.

[6] OpenID Connect Core 1.0. Available at: http://openid.net/specs/openid-connect-core-1_0.html. [Accessed: March 2017].

[7] Infoworld. Millions of embedded devices use the same hard-coded SSH and TLS private keys. Available at: http://www.infoworld.com/article/3009667/security/millions-of-embedded-devices-use-the-same-hard-coded-ssh-and-tls-private-keys.html. [Accessed: March 2017].

[8] Hacker News. Millions of IoT Devices Using Same Hard-Coded CRYPTO Keys. Available at: http://thehackernews.com/2015/11/iot-device-crypto-keys.html. [Accessed: March 2017].

[9] ZDnet. Smart meter hacking tool released. Available at: http://www.zdnet.com/article/smart-meter-hacking-tool-released/. [Accessed: March 2017].
[10] S. C. Patel and P. Sanyal, "Securing SCADA systems," in Inf. Manag. Comput. Secur., vol. 16, no. 4, pp. 398–414, 2008.
[11] C. Warmer and K. Kok, "Web services for integration of smart houses in the smart grid," Proc. of Grid-Interop, pp. 1–5, 2009.
[12] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," in IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 5–20, 2013.
[13] ZDnet. Could lax smart meter security blackout the UK? Available at: http://www.zdnet.com/article/could-lax-smart-meter-security-blackout-the-uk/. [Accessed: March 2017].
[14] S. Tanimoto, R. Kinno, M. Iwashita, T. Kobayashi, H. Sato, and A. Kanai, "Risk Assessment of Home Gateway/Smart Meter in Smart Grid Service," Proc. of Int. Congr. Adv. Appl. Informatics, pp. 1126–1131, 2016.
[15] J. Kołodziej, M. G. Jaatun, S. U. Khan, and M. Koeppen, "Security-Aware and Data Intensive Low-Cost Mobile Systems," in Mob. Networks Appl., vol. 18, no. 5, pp. 591–593, 2013.
[16] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and Access Control in the Internet of Things," Proc. of Intl. Conf. on Distributed Computing Systems Workshops (ICDCSW), pp. 588–592, 2012.
[17] W. L. Chin, Y. H. Lin and H. H. Chen, "A Framework of Machine-to-Machine Authentication in Smart Grid: A Two-Layer Approach," in IEEE Communications Magazine, vol. 54, no. 12, pp. 102-107, 2016.
[18] N. Saxena; B. J. Choi, "Integrated Distributed Authentication Protocol for Smart Grid Communications," in IEEE Systems Journal, pp.1-12, 2016.
[19] N. Mohammad, A. Barua, and M. A. Arafat, "A smart prepaid energy metering system to control electricity theft," Proc. of ICPEC, pp. 562–565, 2013.
[20] N. Tangsunantham, S. Ngamchuen, V. Nontaboot, S. Thepphaeng, and C. Pirak, "Experimental performance analysis of current bypass anti-tampering in smart energy meters," Proc. of ATNAC, pp. 124–129, 2013.
[21] P. Kadurek, J. Blom, J. F. G. Cobben, and W. L. Kling, "Theft detection and smart metering practices and expectations in the Netherlands," Proc. of IEEE ISGT Europe, pp. 1–6, 2010.
[22] T. Fraser. "LOMAC: Low Water-Mark Integrity Protection for COTS Environments," Proc. of IEEE S&P, pp. 230-245, 2000.
[23] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, "TyTAN: tiny trust anchor for tiny devices," Proc. of DAC, pp. 1–6, 2015.
[24] A. R. Al-Ali and M. AL-Rousan, "Java-based home automation system," in IEEE Trans. Consum. Electron., vol. 50, no. 2, pp. 498–504, 2004.
[25] M. G. Golzar and H. Tajozzakerin, "A New Intelligent Remote Control System for Home Automation and Reduce Energy Consumption," Proc. of Asia Int. Conf. on Mathematical/Analytical Modelling and Computer Simulation, pp. 174–180, 2010.
[26] I. Korkmaz, S. K. Metin, A. Gurek, C. Gur, C. Gurakin, and M. Akdeniz, "A cloud based and Android supported scalable home automation system," in Comput. Electr. Eng., vol. 43, pp. 112–128, 2015.
[27] Haowen Chan and A. Perrig, "Security and privacy in sensor networks," in Computer, vol. 36, no. 10, pp. 103–105, 2003.
[28] The hacker News. "Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies" Available at: http://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html. [Accessed: March 2017].
[29] Jixuan Zheng, D. W. Gao, and Li Lin, "Smart Meters in Smart Grid: An Overview," Proc. of IEEE GreenTech, pp. 57–64, 2013.
[30] D. F. Ramírez, S. Céspedes, "Routing in Neighborhood Area Networks: A survey in the context of AMI communications," in Journal of Network and Computer Applications, Volume 55, pp. 68-80, 2015.
[31] Dark Reading. Smart Meter Hack Shuts Off The Lights. Available at: http://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242. [Accessed: March 2017].
[32] M. Weiss, A. Helfenstein, F. Mattern, and T. Staake, "Leveraging smart meter data to recognize home appliances," Proc. of IEEE PerCom, pp. 190–197, 2012.
[33] K. K. J. Biba, "Integrity Considerations for Secure Computer Systems," Proc. of Symposium on Computer Architecture., vol. 5, no. 7, p. 66, 1977.
[34] A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, "An IdM and Key-based Authentication Method for providing Single Sign-On in IoT," Proc. of IEEE GLOBECOM, pp. 1–6, 2015.
[35] D. Drotos. "µCSim: Software Simulator for Microcontrollers," Available at: http://mazsola.iit.uni-miskolc.hu/~drdani/embedded/ucsim/ [Accessed: March 2017].
[36] "IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads," in IEEE Std 2030-2011, pp.1-126, 2011.
[37] M. Wolkerstorfer, B. Schweighofer, H. Wegleiter, D. Statovci, H. Schwaiger, W. Lackner, "Measurement and simulation framework for throughput evaluation of narrowband power line communication links in low-voltage grids," in Journal of Network and Computer Applications, vol. 59, pp. 285-300, 2016.
[38] ANSI, X9 Encryption Collection. Available at: http://webstore.ansi.org/RecordDetail.aspx?sku=X9+Encryption+Collection. [Accessed: March 2017].
[39] Vaadin, OpenID Integration. Available at: https://vaadin.com/directory#!addon/openid-integration. [Accessed: March 2017].
[40] Java API for RESTful Services. Available at: https://jax-rs-spec.java.net/. [Accessed: March 2017].
[41] Eclipse Foundation, "Californium." Available at: https://www.eclipse.org/californium/. [Accessed: March 2017].
[42] The Contiki Operating System. Available at: http://contiki-os.org/. [Accessed: March 2017].
[43] A. Mohammadali, M. H. Tadayon, and M. Asadian, "A new key management for AMI systems based on DLMS/COSEM standard," Proc. of Int. Symp. Telecommun., pp. 849–856, 2014.
[44] R. Ribeiro, A. Santin, V. Abreu, J. Marynowski and E. Viegas. "Providing Security and Privacy in Smart House Through Mobile Cloud Computing," Proc. of IEEE Latin-American Conference on Communications, pp. 1-6, 2016.
[45] E. Niewiadomska-Szynkiewicz, A. Sikora, and J. Kołodziej, "Modeling mobility in cooperative ad hoc networks," in Mob. Networks Appl., vol. 18, no. 5, pp. 610–621, 2013.