future internet

Article

Smart Devices Security Enhancement via Power Supply Monitoring [†]

Dimitrios Myridakis [1,*], Georgios Spathoulas [1], Athanasios Kakarountas [1,*] and Dimitrios Schinianakis [2]

[1] Department of Computer Science and Biomedical Informatics, University of Thessaly, 35131 Lamia, Greece; gspathoulas@dib.uth.gr

[2] Cyber Security Munich (CSM), NOKIA Bell Labs, 81541 Munich, Germany; dimitrios.schoinianakis@nokia-bell-labs.com

[*] Correspondence: dmyridakis@dib.uth.gr (D.M.); kakarountas@uth.gr (A.K.)

[†] This paper is an extended version of our paper published in proceedings of 2019 15th International Conference on Distributed Computing in Sensor Systems, titled "Monitoring Supply Current Thresholds for Smart Device's Security Enhancement".

Received: 21 January 2020; Accepted: 7 March 2020; Published: 10 March 2020

Abstract: The continuous growth of the number of Internet of Things (IoT) devices and their inclusion to public and private infrastructures has introduced new applciations to the market and our day-to-day life. At the same time, these devices create a potential threat to personal and public security. This may be easily understood either due to the sensitivity of the collected data, or by our dependability to the devices' operation. Considering that most IoT devices are of low cost and are used for various tasks, such as monitoring people or controlling indoor environmental conditions, the security factor should be enhanced. This paper presents the exploitation of side-channel attack technique for protecting low-cost smart devices in an intuitive way. The work aims to extend the dataset provided to an Intrusion Detection Systems (IDS) in order to achieve a higher accuracy in anomaly detection. Thus, along with typical data provided to an IDS, such as network traffic, transmitted packets, CPU usage, etc., it is proposed to include information regarding the device's physical state and behaviour such as its power consumption, the supply current, the emitted heat, etc. Awareness of the typical operation of a smart device in terms of operation and functionality may prove valuable, since any deviation may warn of an operational or functional anomaly. In this paper, the deviation (either increase or decrease) of the supply current is exploited for this reason. This work aimed to affect the intrusion detection process of IoT and proposes for consideration new inputs of interest with a collateral interest of study. In parallel, malfunction of the device is also detected, extending this work's application to issues of reliability and maintainability. The results present 100% attack detection and this is the first time that a low-cost security solution suitable for every type of target devices is presented.

Keywords: internet of things; hardware security; anomaly detection; smart device; current monitoring; physical characteristics

1. Introduction

Successful attacks targeting Internet of Things (IoT) smart devices have been reported [1–3] in many research works presented in recent years. This raises significant security issues and sets new challenges. The security issues concern the personal safety of civilians and the security of their equipment, as well as the protection of other digital infrastructures from a potential botnet attack. On the other hand, there are challenges in confronting successful attacks originating from botnets populated of hijacked IoT devices. The number of attacks is increasing exponentially each year, in analogy to the vulnerabilities they exploit, and most of the time, with unpredictable results. The characteristics of the attacks vary significantly from attack to attack and from time to time. The warnings for the severity of the attacks [4] indicate that there is a need for solutions addressing attacks from birth. Moreover, following protocols similar to the pandemic spread of a biological virus, there is a need to quarantine infected IoT devices, thus prohibiting the spread of the infection and thus the formation of the botnet. However, this is difficult since there is no previous knowledge of a new virus, or the vulnerabilities of a smart device. Finally, since there is physical access to smart devices, there is even the threat of software alteration just by swapping the device's memory card.

In addition to the previously mentioned security issues, there is the need to monitor normal operation of our equipment. This includes operation time, power dissipation and many more. It is desirable to detect any anomaly on time in order to avoid electrification or permanent destruction of our equipment. Issues like electronic ageing, physical degradation of materials, etc., may create significant difference in characteristics of operation without being evident in due time.

This work is an extended version of [5] and presents a new concept for the identification of an anomaly created by a virus attack to an IoT device or by the damage of a capacitor in the electronic device. The work leverages lessons learned from side-channel attack technique and specifically, power analysis [6]. This implies that power analysis may serve as a unique signature of the executed code. Since an IoT device executes usually only one well defined task, it turns out that the behavious (operation) of an executed code may be easily analyzed [7]. Furthermore, since this behaviour is defined by the processing components of the device utilized by the executed code, then the overall power dissipation during normal operation varies in an explicit range. Thus, during normal operation, we expect the device's power dissipation to be found in this safe range. Since such a device may have several operation modes (e.g., normal operation, update, sleep mode, etc.) it is possible to extend the safe range to include several ranges, forming clusters of operation. Thus, any power deviation, caused by either increased traffic to the network or an internal anomaly (Trojan hardware or software virus) is expected to be detected.

This work is organized as follows. In Section 2, an exploration of related work is offered and in Section 3, the proposed approach to detect an IoT device's anomalous operation is presented. Then, in Sections 4 and 5, the experiments and the results from the implementation of a prototype are presented. Finally, in Section 6, the paper is concluded.

2. Related Work

A significant number of research efforts, presented through the last years, have been related to IoT devices and issues related to their operation. A number of works that reflect the research have been conducted recently, regarding IoT devices and issues regarding security and availability. The most important issues that were depicted from the conducted study were the reliability (directly associated with availability) and the security of IoT devices.

The reliability of IoT devices is significant and can be affected by various factors such as the operational environment, the manufacturing process (genuine or counterfeit, trojan hardware) [8] and the faulty condition of the device itself (malfunctioning, transient errors, etc.) [9]. In general, works associating availability with the operation of IoT highlight hardware as a key point. Although, this issue of reliability is critical for numerous applications, researchers usually study it only theoretically or under laboratory conditions. Reliability, however, is extremely prone to operational conditions [10] and needs to be further investigated. What is very interesting as a case study is the study of similar (or identical) smart devices operating under various conditions (normal to extreme) and the calculation of the degradation of reliability (as a metric) based on the Mean Time Before Failure (MTBF) for each environment. However, apart from this case study, which is typical for expected conditions of operation, there are cases when hardware is not operating as expected. Such cases include the effect of a Trojan hardware, or a side channel attack. Taking lessons from other disciplines like circuit testing, at the beginning of the anomalous operation, this resembles the effect of the Single Event Upset (SEU) [11]. Thus, many hardware anomalous operations may be characterized as deviations of the characteristic operation.

Concerns software of an IoT device, the detection of an execution of a malicious code or the effect of an attack is different. Although, in the past, computing machines were based on similar architectures and their implementations resulted in bulky systems, using complex design methodologies, the process to protect them and generally ensure security was feasible. Nowadays, the diversity of IoT devices along with their shrinking processing capabilities have made their protection a very hard task. Regarding security issues, the recent growth in usage of heterogeneous computing devices [12] has made the protection of a computing infrastructure against all kind of risks, such as cyber-attacks, malfunctioning or privacy leaks, much more difficult [13,14]. A lot of recently reported cyber-security problems are directly or indirectly related to the unprecedented switch in the form of today's devices. As a consequence, IoT devices have been recently used to construct massive botnets and execute distributed denial of service attacks, the size of which is larger than that of any known attack in the past [15,16]. In practice, the insufficient security measures that the vendors usually implement on such devices actually extend the attack surface, offering new opportunities in terms of building more efficient botnets.

Additionally, the acquisition and the nature of data processed by these devices constitutes an important privacy threat for users [17,18]. IoT devices, installed at work or even in public places, monitor and store data relevant to the activities happening in their observation space. In practice, an IoT device collects data relevant to the activity of the people present in these spaces, sometimes even without their consent or even knowledge. The monitoring, storing, processing or even use for profit of such data, has serious privacy implications for the people involved. The market for producing IoT devices is growing exponentially. Multiple new vendors claim a share of this market, introducing new IoT devices of various configurations and features. This has direct implications on the quality of new IoT devices. In a market of cheap devices but high-volume production, vendors usually opt for the most competitive product that is low cost and has a short time-to-market. Thus, security is not the most important factor for such low-priced devices. This results in the introduction to the market of less secure products, or their alternatives, due to the need for low cost [19,20].

Another important factor that intensifies the problem is that a significant percentage of IoT devices already in use, especially in industrial installations, are devices that were not designed with internet connectivity in mind. Changes in requirements or ease-of-use reasons have forced people to connect such installations to the internet. In almost all such cases, these devices have not been reconfigured in order to be protected [21]. This may happens either due to insufficient security awareness or due to the fact that the specific devices are simply not reconfigurable. This has led to important industrial security breaches [22].

Finally, a new approach was presented by Myridakis et al. in [5,7] which considers the extracted information from the supply current as appropriate for detect operational anomalies of the IoT devices (either using threasholds or ranges of values). An extension of this approach was also considered by Papafotikas et al. in [23], who proposed a self-learning system that profiles normal operation in clusters and any operation outside them is detected as anomalous operation.

3. Proposed Side-Channel Monitoring Device

The main idea of the present paper was the monitoring of the supply current in order to detect abnormal operation of IoT devices. The concept is based on the fact that any operation of an electrical and electronic device is characterized by its consumption. Furthermore, considering that power consumption depends on the input characteristics, it may be concluded that a system performing an explicitly defined operation is bounded in a characteristic power consumption range. Considering that IoT devices are limited in terms of functionality and operational features, it is expected that any deviations from normal operation will result in analogous deviations regarding the consumed power.

Thus, any malicious action against the IoT device is expected to be detected via the power consumption deviation caused by the malicious attack source.

The contribution of this paper is the introduction of an external mechanism to the IoT devices, which has a generic use and is easily adaptable to any IoT device. This mechanism is a power supply monitoring system specifically designed for the targeted device which analyzes the device's electrical behaviour without affecting its operation. This can provide a good indication regarding the possibility that the device operates in an abnormal way. It is expected that deviations in the network or processing activity of the IoT device will trigger analogous deviations regarding energy consumption. Since the electrical behaviour of the IoT device is stored to the external monitoring system, any effect of a malicious attack to the IoT device may not be masked by the attacker. Violation of normal operation thresholds are triggering the detection of the attack. Throughout this work, the pre-characterization of the normal operation thresholds of the supply current is performed by the user. In the last section of this work, the future work reveals the next steps towards an automatic set of the normal operation supply current range.

In this paper, we set up a device as an intermediate observer between the device that we want to monitor and its power supply. This approach is realistic since all devices offer access to their power supply. The proposed system can be eventually used to detect reliability problems and security-related attacks against the device. The constructed setup as well as the relative measurement data are presented throughout the rest of the paper.

The topology of a final solution is presented in Figure 1, where any home connected to the Internet may use the services of an IDS provider. To date, a botnet of smart devices attacks either the IDS or the targeted device. The second scenario is in the scope of this paper. Each smart device is connected to the energy grid (power supply) via the proposed monitoring devices and to the Internet via the router. Any deviation from the expected operation is reported to the IDS and at the same time, fail safe procedures may be triggered, based on security policies. In this work, research was focused only on anomaly detection.

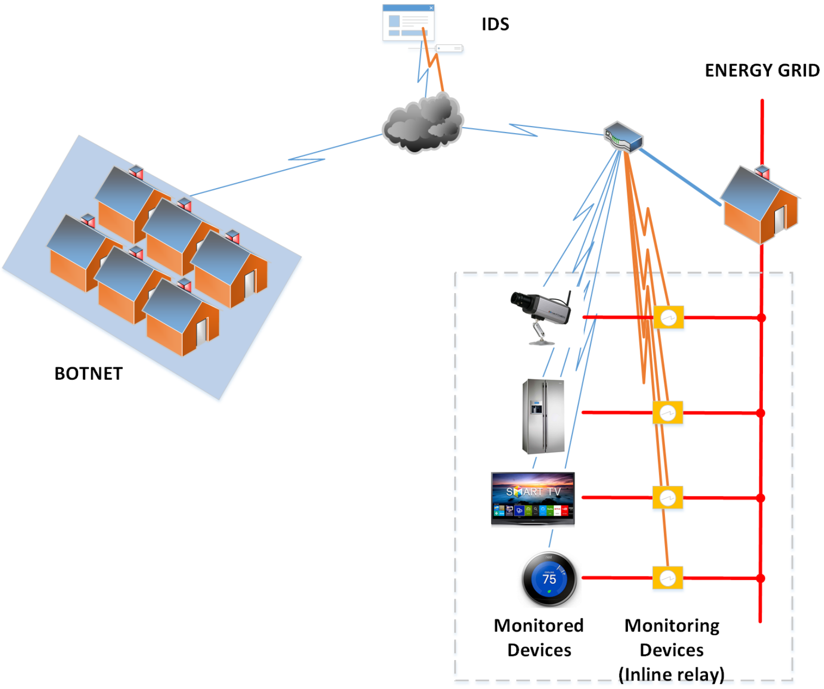

Figure 1. Topology of the monitoring devices in a household.

Proposed Setup

In order to implement the proposed setup, we assembled, as the target device, a custom IP camera and used a low-cost micro-controller to monitor the power energy amperage of the targeted device. As a target device, we created an IP camera on a programmable micro-computer appropriate for our purposes. The micro-controller device was interposed between the power supply and the monitored device. The clarification is as follows:

- The monitoring circuit includes a 1 Ohm resistor and a smaller calibrating resistor used for accuracy reasons. The resistor is located between the two inputs of the micro-controller in order to measure the amperage. The power amperage can be calculated through the measurement of the voltage at the two input points according to the following formula:

$$I = \frac{V_2 - V_1}{R} \tag{1}$$

  where V_1 and V_2 are the two reference voltages as depicted in Figure 2, and R is the 1 Ohm resistor.
- Two analog inputs of the micro-controller are connected to the circuit (Figure 2) in order to collect the power measurements. The first input is connected to the point before the resistor while the second is used to measures the voltage at the other end of the resistor.
- Finally, the device to be monitored is connected serially to the resistor. The circuit is completed by connecting an Alternating Current (AC) power supply 5 V for the power jack.

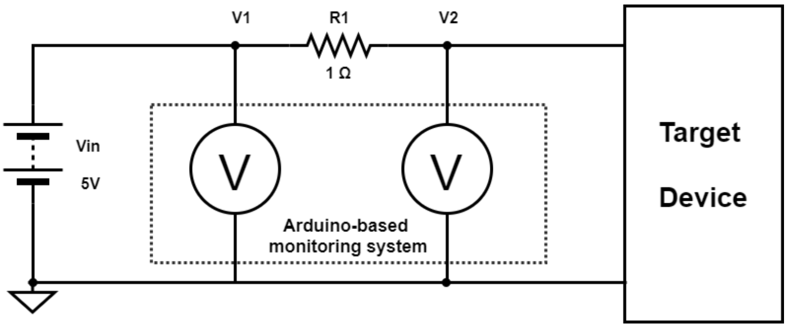

Figure 2. Circuit of Monitoring Device.

Additionally we improved the Signal-to-Noise Ratio (SNR or S/N) with a software technique. The monitoring device may be easily programmed and thus, a moving window algorithm was exploited to smoothen the signal deviations. Thus, spikes may be eliminated when occurring rarely, while a more frequent appearance of spikes is preserved for anomaly detection. This signal smoothing technique is called the moving average. From the raw data sequence [y_1, y_2, ..., y_N], we created a corresponding smoothed data sequence. The smoothed point $(y_k)_s$ is the mean of an odd number 2n + 1 (n = 1, 2, 3, ...) of the raw data sequences $y_{k-n}, y_{k-n+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+n-1}, y_{k+n}$, i.e.,:

$$(y_k)_s = \sum_{i=-n}^{i=n} y_{k+i}/(2n+1) \tag{2}$$

The odd number 2n + 1 is the window width. The larger the window width, the more intense the smoothing. The SNR can be further enhanced by increasing the window width or by multiple window passes (smoothing at already smoothed points). During average moving window processing, a spike calculation is also conducted, comparing value y_k to the thresholds $y_{thres.max}$ and $y_{thres.min}$. Let us assume that the spike is positive, that is, the signal is ascending; then, sp_k is set to 1 only in case y_k is greater than $y_{thres.max}$. The sp_k is also set to 1 in case the spike is negative, that is, the signal is descending and the y_k is less than $y_{thres.min}$. Then, the final population of spikes is calculated in a time window including an odd number of samples, e.g., 2*m*+1, where *m*»*n*.

$$sp_k = \begin{cases} 1 & \text{if } y_k > y_{thres.max} \text{ and } y_k - y_{k-1} > 0, \\ 1 & \text{if } y_k < y_{thres.min} \text{ and } y_k - y_{k-1} < 0, \\ 0 & \text{if } otherwise \end{cases} \quad (3)$$

where the *k*-th sample has a value of y_k, which is compared to the appropriate threshold $y_{thres.max}$ or $y_{thres.min}$, respectively, to its previous value. The calculation is performed for 2*m*+1 samples y_{k-m}, y_{k-m+1}, ..., y_{k-1}, y_k, y_{k+1}, ..., y_{k+m-1}, y_{k+m}, where *m*»*n*. Then, a rough estimation of the identified spikes in the 2*m*+1 consecutive samples is performed with the following equation:

$$spikes = \sum_{i=-m}^{i=m} sp_{k+i} \quad (4)$$

The selection of *m*, *n*, $y_{thres.max}$ and $y_{thres.min}$ in this work was considered as information given by the manufacturer of the IoT device. The typical value for *m* is 5000 and for *n*, it is 20. The *spikes* that set an alarm were selected to be 50 in order to avoid negative positives due to random spikes originating from the energy grid.

4. Experiments

In order to prove the concept of this work, we set as a target to detect anomalies in normal operation of a device by monitoring its supply current deviations. Any deviation is a warning for the presence of a potential anomaly. The detection factor is a violation of the normal operation thresholds for a selected time period. Although this time period was derived empirically, in a future version of the monitoring device, it is expected to be derived automatically by an embedded machine learning algorithm. The expected operation will be referenced hereinafter as the normal profile of the device.

Three scenarios were considered in order to check various types of anomalous operation that occur from malicious attacks. The first scenario assumes a custom made smart thermometer measuring temperature and humidity in a house. The anomalous operation is simulated by replacing the sensor with one which was taken from the damaged materials of our laboratory (which was hypothetically destroyed by an attacker—physical attack to the system). The expected result should present a systematic error over time. The current thresholds were measured for normal operation in the temperature range 10 °C–30 °C. The damaged sensor that was chosen presented permanent stuck-at-1 faults in several output bits. The second scenario assumes a custom smart security camera installed at a home. An attack is performed via the network, attempting to take control of the device by simulating a bot attack. The third scenario assumes physical access to a camera (physical attack by replacement of the equipment with an infected one) and swapping of the memory card with another one with a pre-installed infected application code.

4.1. Evaluation of Measurement Validity

In order to evaluate the validity of the measurements, a digital multimeter was incorporated to measure voltage and supply current at the same nodes. The tests were repeated and the measurements acquired by the digital multimeter and our custom monitoring setup were compared. The results have negligible deviations from those of the digital multimeter, as expected in the bounds of the instrument error.

4.2. Experiment's Set-up

In order to prove that the anomaly detection is feasible, the following set-ups were followed. For the first scenario, the smart thermometer, which consists of an Arduino Uno Rev3 microcontroller with a built-in Wi-Fi shield, and a DHT 22 sensor for measuring temperature and humidity in the house, were placed in a home. Measures were taken to eliminate all sources of deterioration in the home environment.

For the second scenario, a Denial of Service (DoS) attack was employed through the use of hping3 script on the IP camera target device, which consisted of a Raspberry Pi 3 B+ microcontroller as well as a RPI 8MP camera board version 2. Two different monitoring periods were employed. During the first period, which lasted for a week, the camera was operated normally without any attack being executed against it. The second monitoring period lasted 24 hours and during that time, three different DoS attempts were executed against the camera. The three attacks occured as per the following timetable:

- The first attack was between 06:00 and 07:00.
- The second attack was between 14:30 and 15:30.
- Finally, the third attack took place between 21:30 and 23:00.

For the third scenario, we followed the same setup as that of the first scenario, that is, controlled external conditions without any sources of physical effects. The difference is found solely in the infected software executed on the same hardware.

For all the scenarios and the profile measurement experiments, the supply current sampling period was 100 ms. This was derived by the operating frequency of the IoT devices.

5. Results

In this section, the results acquired by the devices during the experiments are depicted. The time period of the samples is adequate to present the results of the detected anomaly. Using simple rules of thresholds or range of values, anomaly detection is achieved only by one physical parameter of operation, that is, the supply current. An analysis of the results and the values is presented for each scenario separately in the following subsections.

5.1. First Scenario—Smart Thermometer

For the first scenario, regarding the smart Thermometer, the device performed its normal operation by capturing temperature and room humidity. Regarding the first scenario, two profiles were considered:

5.1.1. Normal Profile

In this operation profile, an external environmental factor did not exceed normal characteristics and an attack was not performed, in order to have a profile-reference of normal conditions and good equipment. In Figure 3, the supply current that was measured during 350 s is depicted.

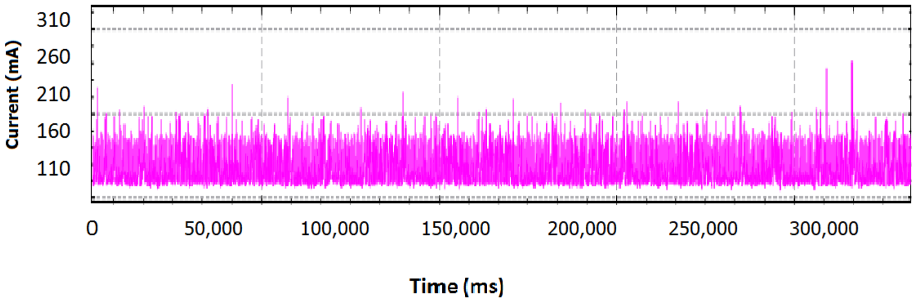

Figure 3. Smart thermometer normal profile.

5.1.2. Anomalous Profile

In this operation profile, the sensor was removed and replaced with a damaged one. The captured values for 350 s, show in Figure 4, that there is a notable variation of the measured supply current. This happens due to the stack-at-1 faults of the damaged sensor, which create a higher power dissipation of the proposed monitoring device's ADC (Analog to Digital Converter). Exploiting this finding, and taking into consideration the spike count, the monitoring mechanism can detect efficiently such a behaviour. It should be noted that this detection is feasible only if the stack-at-1 faults drastically affect the ADC power consumption and the number of spikes exceeding the thresholds is high enough to determine a deviation in operation.

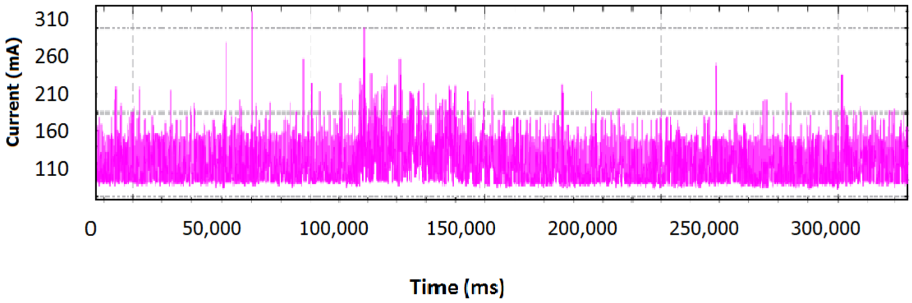

Figure 4. Smart Thermometer with damaged sensor.

5.2. Second Scenario—IP Camera under DoS Attack

A Raspberry Pi (IP Camera), along with a Arduino Uno (monitoring circuit), were placed in a dummy camera enclosure to produce a usable device. Regarding the second scenario, two profiles were considered again.

5.2.1. Normal Profile

In this scenario, the microelectronic device performed periodical capturing of current values. An external environment factor did not exceed normal characteristics and an attack was not performed, in order to construct a baseline profile of the power amperage under normal conditions' operation for comparison reasons. This profile (Normal) is depicted in Figure 5, showing three charts in time (hours) on the horizontal axis. In Figure 5A the supply current of the device is displayed as measured by the external circuit. In Figure 5B the smoothing filter was applied, where the power fluctuations is distinguished, and finally, in Figure 5C, the second pass from the same filter is offered.

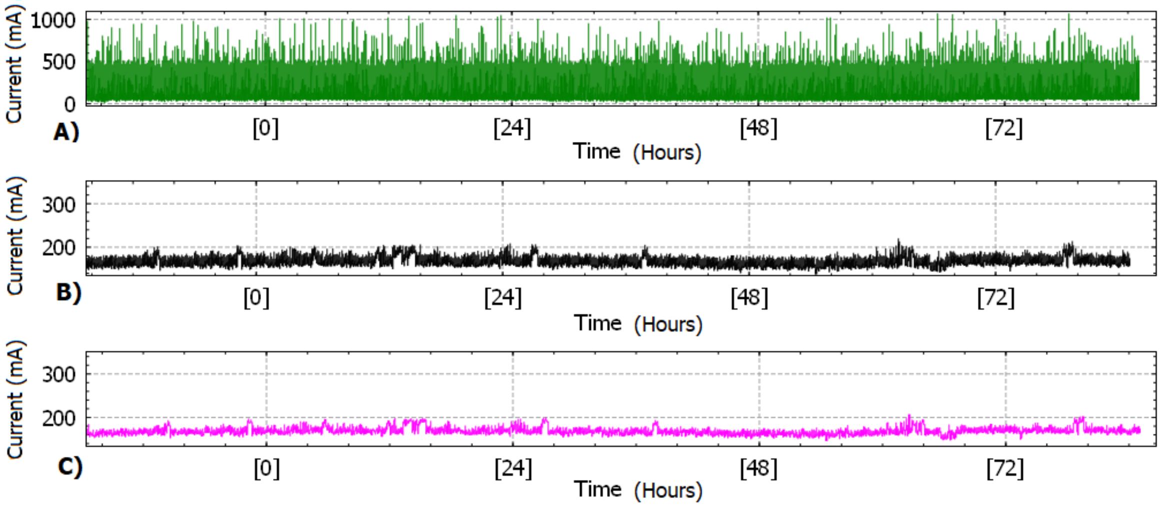

Figure 5. Measurement during operation without attacks (Normal Profile) [5].

5.2.2. Anomalous Profile

In this scenario, a DoS attack was performed against the device, while its normal functionality was executed: collecting data. The measurements regarding supply current were captured in order to observe the device's network activity and the values are depicted in Figure 6.

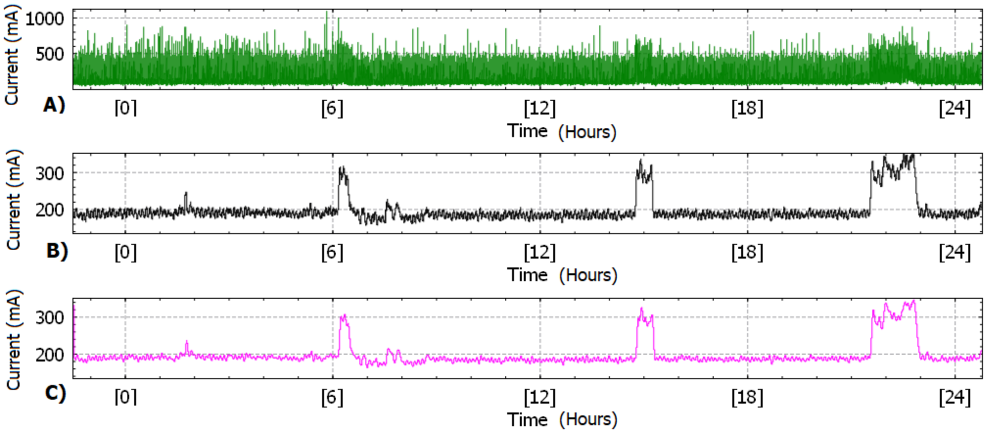

Figure 6. Measurement of operation under attack (Anomaly Profile) [7].

In Figure 6A, there is indeed a deviation (spikes) of current supply when there is a DoS attack. Considering that the features of the DoS attack were realistic, it may be said that even with a simple external monitoring system, it is possible to detect an operational anomaly. It is expected to measure even bigger deviations under a massive Botnet attack and thus trigger a safe mode for the smart device. Even by applying the smoothing filter, as seen in Figure 6B,C (one pass and two passes respectively), the number of spikes, as calculated by Equation (4), is high.

5.3. Third Scenario—IP Camera with Infected Code

For the last scenario, an IP camera was used (exploiting the equipment of the second scenario) for security reasons. This scenario assumes that there is physical access to the equipment and that the attack is the replacement of the memory card with another one installed with infected code. More specifically, the mirai malware code was added to the camera card. That is a copy of the initial OS and the application code, including, however, the Trojan horse. This scenario proves that the external monitoring system will detect abnormal behavior even if there is no network attack, but rather, an implicit malicious attack, that is, the change of the equipment with an infected one. Again, two profiles were considered.

5.3.1. Normal Profile

In this operation profile, neither an external environmental factor exceeded normal characteristics nor an attack was performed, in order to have a profile of normal conditions for reference values. The supply current samples for 350 seconds are depicted in Figure 7.

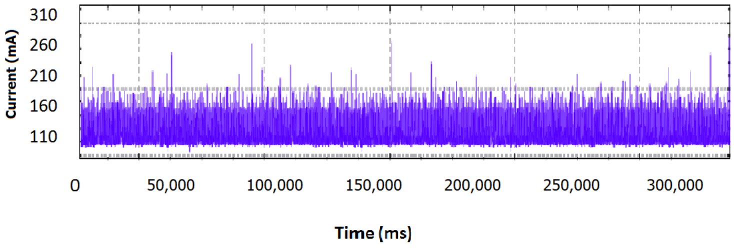

Figure 7. IP Camera Normal Profile.

5.3.2. Anomalous Profile

In this operation profile, the memory card was removed and replaced with an infected one. The captured values prove that there is a measurable variation in the measured current. The triggering of the malicious code resulted in excessive power consumption, which is depicted in Figure 8. Again the number of spikes, as calculated by Equation (4) is high and the notable deviation is easily detected.

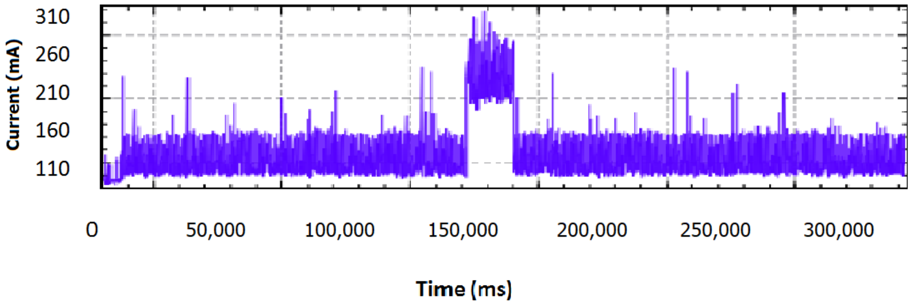

Figure 8. IP camera with infected application code.

6. Conclusions

In this work, the introduction of a solution for monitoring IoT devices exploiting characteristics of the side-channel attacks is presented. The idea is based on the fact that manufacturers do not provide security mechanisms or hacker countermeasures in their IoT products, mainly due to their low cost. However, this leads to a critical increase of the security surface that needs to be protected. Successful attacks to IoT devices are announced every day but the main actions to secure the IoT devices are mainly found in commercial Intrusion Detection Systems (IDS). Furthermore, attacks have become more sophisticated, and are able to mask themselves from IDS discovery.

The concept follows the assumption that any additional data processing will lead to an increase in power consumption. Thus, a monitoring mechanism was developed using a simple circuit and a microcontroller able to perform simple calculations and be placed between the power plug and the IoT device. The continuous monitoring of the supply current for a device with explicitly defined operation may reveal significant information and expand data for the status of the IoT device. The latter is significant for the modern IDS, and it generally follows bio-inspired approaches for anomaly detection.

Hence, the supply current was monitored by exploiting knowledge gained from side-channel attacks. The deviation of the monitored current was correlated to security and reliability issues of IoT devices and it was proven that an anomaly may be detected with non typical methods. The main contribution of this work is that it introduced a new technique to detect operational anomalies of smart devices in a symptomatic approach rather than by identifying the cause itself. This allows on-time anomaly detection, a decrease of security dependency from the targeted IoT device and an increase of the data that may be correlated to a new kind of botnet.

The extension of monitored parameters for security issues confronted by IDS is expected to be integrated soon in major systems. The presented method is the basis for this type of parameter extension that will provides additional measurements for protecting critical IoT infrastructures. The handling of the collected data in an IDS and the exploitation of Machine Learning (ML) algorithms in order to identify promptly new kinds of attacks, will be challenges for future research. This work may be expanded by automating the process to define the normal operational thresholds and the calculation of the sufficient number of spikes to efficiently detect anomalies and finally, the dynamic definition of variables m and n. Finally, although the technique has decent performance regarding the reliability of the equipment (in contrast to the network attack and the physical attack), it may be used as a means to detect hardware Trojans or IP counterfeits.

Author Contributions: Conceptualization, A.K.; methodology, A.K., D.M. and G.S.; software, D.M.; validation, D.M.; investigation, D.M.; resources, D.S.; data curation, D.M.; writing–original draft preparation, A.K. and D.M.; writing–review and editing, G.S. and D.S.; visualization, D.M.; supervision, A.K.; project administration, A.K.; funding acquisition, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by NOKIA Bell Labs through global donation program for "Research on IoT Security based on Bio-informatics".

Acknowledgments: The authors would like to acknowledge the contribution of Joachim Lueken through creative discussions during the last two years. We would also like to acknowledge the professional assistance of the MDPI Future Internet personnel throughout the review process and the reviewers for their numerous comments, who have helped us improve significantly the submitted manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AC	Alternating Current
ADC	Analog to Digital Converter
DoS	Denial of Service
IDS	Intrusion Detection Systems
IoT	Internet of Things
MTBF	Mean Time Before Failure
ML	Machine Learning
SEU	Single Event Upset
SNR	Signal-to-Noise Ratio

References

1. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
2. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 Feburary 2017; pp. 32–37.
3. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
4. Sapienza, A.; Bessi, A.; Damodaran, S.; Shakarian, P.; Lerman, K.; Ferrara, E. Early warnings of cyber threats in online discussions. In Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW), New Orleans, LA, USA, 18–21 November 2017; pp. 667–674.
5. Myridakis, D.; Spathoulas, G.; Kakarountas, A.; Schinianakis, D.; Lueken, J. Monitoring Supply Current Thresholds for Smart Device's Security Enhancement. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 224–227. [CrossRef]
6. Liu, Y.; Wei, L.; Zhou, Z.; Zhang, K.; Xu, W.; Xu, Q. On code execution tracking via power side-channel. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1019–1031.
7. Myridakis, D.; Spathoulas, G.; Kakarountas, A.; Schoinianakis, D.; Lueken, J. Anomaly detection in IoT devices via monitoring of supply current. In Proceedings of the 2018 IEEE 8th International Conference on Consumer Electronics-Berlin (ICCE-Berlin), Berlin, Germany, 2–5 September 2018; pp. 1–4.
8. Kitsos, P.; Sklavos, N.; Voyiatzis, A.G. Ring oscillators and hardware Trojan detection. In *Hardware Security and Trust*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 169–187.
9. Keramidas, G.; Voros, N.; Hübner, M. *Components and Services for IoT Platforms: Paving the Way for IoT Standards*; Springer: Berlin/Heidelberg, Germany, 2016.
10. Smith, D.J. *Reliability, Maintainability and Risk: Practical Methods for Engineers*; Elsevier: Amsterdam, The Netherlands, 2017.

11. Morgan, K.; Caffrey, M.; Graham, P.; Johnson, E.; Pratt, B.; Wirthlin, M. SEU-induced persistent error propagation in FPGAs. *IEEE Trans. Nucl. Sci.* **2005**, *52*, 2438–2445. [CrossRef]
12. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
13. Lee, Y.; Kim, D. Threats Analysis, Requirements and Considerations for Secure Internet of Things. *Int. J. Smart Home* **2015**, *9*, 191–198. [CrossRef]
14. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Int. Res.* **2016**, *26*, 337–359. [CrossRef]
15. Angrishi, K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. *arXiv* **2017**, arXiv:1702.03681.
16. Dobbins, R. Mirai IoT botnet description and DDoS attack mitigation. *Arbor Threat Intell.* **2016**, *28*.
17. Porambage, P.; Ylianttila, M.; Schmitt, C.; Kumar, P.; Gurtov, A.; Vasilakos, A.V. The quest for privacy in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 36–45. [CrossRef]
18. Ziegeldorf, J.H.; Morchon, O.G.; Wehrle, K. Privacy in the Internet of Things: threats and challenges. *Secur. Commun. Netw.* **2014**, *7*, 2728–2742. [CrossRef]
19. Li, H.; Liu, Q.; Zhang, J. A survey of hardware trojan threat and defense. *Integr. VLSI J.* **2016**, *55*, 426–437. [CrossRef]
20. Moein, S.; Gulliver, T.A.; Gebali, F.; Alkandari, A. A new characterization of hardware trojans. *IEEE Access* **2016**, *4*, 2721–2731. [CrossRef]
21. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial Internet of Things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.
22. Langner, R. Stuxnet: Dissecting a cyber-warfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
23. Papafotikas, S.; Kakarountas, A. A Machine-Learning Clustering Approach for Intrusion Detection to IoT Devices. In Proceedings of the 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Piraeus, Greece, 20–22 September 2019. doi:10.1109/SEEDA-CECNSM.2019.8908520. [CrossRef]