Proceedings of the 2021 International Conference on Information Technologies (InfoTech-2021), IEEE Conference, Rec # 52438
16-17 September 2021, St. St. Constantine and Elena, Bulgaria

A model for identification of compromised devices as a result of cyberattack on IoT devices

Aleksandar Hristov and Roumen Trifonov
Department "Information technologies in industry", Faculty of Computer Systems and Technologies
Technical University of Sofia
8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria
ahristov@tu-sofia.bg, r_trifonov@tu-sofia.bg

Abstract – **The present paper aims to propose an intelligent system for identification of compromised Internet of Things (IoT) devices due to cyberattack, using Wavelet transformation and Haar filter. Monitoring is being made and the state is identified through time-synchronized series of indexes for usage of processor, memory and network interface card. Using system monitor the time-synchronized indexes of non-compromised IoT devices are saved as well as indexes of compromised IoT devices due to some well-known cyberattacks in Internet of Things are saved. The parameters of the proposed system are being specified in order to distinguish (filter) the two states of the IoT devices (non-compromised or compromised) by these indexes.**

Keywords – **Artificial Intelligence Systems, Information Security, Internet of Things, IoT devices, Wavelet transformation.**

I. INTRODUCTION

Nowadays information and communication technologies are becoming the basis of all our activities: economics, administration and private life. Digital infrastructures [1] are becoming a key factor for the management and proper functioning of all resources and systems of national importance, the development of a competitive and innovative economy, transparent governance and a modern society.

The interest in the Internet of Things (IoT), the Industrial Internet of Things (IIoT) and in particular the information security [3] of IoT devices is a growing. IoT devices are increasingly being compromised and used in a wide variety of attacks because they often lack critical device protections such as strong passwords, up-to-date operating systems, and segmented networks. Moreover, the specifics of the IoT devices, which are hard or soft real time and Internet services, are important to define the type of attacks that can destroy their functionality.

The review of the literature showed that the problem with information security of IoT devices is still poorly developed and there are no available systems for detecting compromised IoT devices as a result of cyberattack, so we believe that the results will be of national and international importance, considering the National Research Strategy and the challenges set out in it, as well as the institutional and European priorities.

In [4], a specific approach for identifying compromised devices as a result of a cyberattack is proposed. It is based on monitoring the usage of processor, memory and network interface card (NIC) to determine the status (compromised / non-compromised) of IoT devices. The decisive rule (a function dividing the space of two disjoint sets) of the algorithm finds the correspondence of the state from a time series of values as an input. A peculiarity of the approach is the pre-treatment, i.e. using training samples of time series (usage of processor, memory and network interface card), three cluster areas are determined as well as the center of each cluster. The first cluster corresponds to a non-compromised state, while the second and third clusters correspond to states after SQL Injection. For the second cluster filtering by a predefined field of the table is being done and for the third cluster the values are inserted into a table after they have been changed. An advantage of the approach above is that it distinguishes these two specific compromised states, and a disadvantage is that it cannot identify all sorts of other compromised states of the IoT device.

Different approaches are known in the literature [6, 10, 11] for identification of the IoT devices especially in IoT sensor swarms [6 and its references] – some behavioral files are stored and periodically the device must generate the same files that are to be equal to the etalon ones. Mostly cryptography hashing or public key authentication are used.

NIST's NICE [9] includes all the processes necessary to assure that existing and new IT systems meet the organization's cybersecurity and risk requirements. In the NICE Protect and Defend work category it is discussed how to conduct assessments of threats and vulnerabilities; determining deviations from acceptable configurations or policies; assessing the level of risk; and developing or recommending appropriate mitigation countermeasures.

Despite there are several industry standards [9, 11] for IoT identifications in the network hierarchy, there is no uniform standard and this proves the actuality of the problem.

The present paper aims to propose an intelligent system for identification of compromised Internet of Things (IoT) devices due to cyberattack, using Wavelet transformation and Haar filter. This model will be based on analysis of the methods and means of information security systems through applied tools.

II. A UNIVERSAL METHOD FOR IDENTIFYING COMPROMISED STATES

Below it is proposed a universal method for identifying various compromised states of IoT devices. This method

This paper is sponsored by Scientific and research sector, TU-Sofia, contract № 212ПД00001-09

uses coefficients obtained from the Wavelet transformation for the memory usage (in percentage) of the IoT device.

The wavelet transform [5] is a transform that provides both time and frequency representation. It passes the time-domain signal from high pass and low pass filters, which filters out either high frequency or low frequency portions of the signal. Every time this procedure is repeated some portion of the signal, corresponding to some frequencies, is being removed from the signal. The procedure is called decomposition. The decomposition is repeated to a predefined decomposition level. Next, a set of signals is produced which actually represents the original signal. For sampled signals (as in our case) the Discrete Wavelet Transform is used. The Haar transform [5] decomposes a discrete signal into two subsignals of half its length. One subsignal is a running average or trend, T; the other subsignal is a running difference or fluctuation, d.

Since the energy of the trend subsignal T accounts for a large percentage of the energy of the transformed signal, in the following, the energy is computed by considering only the trend coefficients of the first level decomposition as shown in the following equation:

$$E_T = \sum_{j=1}^{n} T_j^2 \quad (1)$$

For memory usage [4] of the IoT device, the Discrete Wavelet Transformation should be used. The method for identifying of various compromised states of IoT devices uses as a metric the energy value of the Wavelet transform [5] for the memory usage.

This method is a two phase process. At the first phase (Initial Phase), the Wavelet energy value of non-compromised IoT device is measured and stored. In the second phase (Test Phase) the Wavelet energy of the tested IoT device is measured and compared to the corresponding reference value. The detection of a compromised IoT device will be successful when its Wavelet energy value exceeds certain tolerance limits. These limits are introduced in order to account for memory usage variations and measurement inaccuracies. Finally, the definitions of the Wavelet energy for the non-compromised IoT device and the tolerance limits along with the percentage detectability values are calculated.

Given an initial set of *n* non-compromised states, set $E_{T,i}$ to be the energy value of the memory usage of IoT device for different non-compromised states, $E_{T,mean}$ the mean Wavelet energy value of all non-compromised states and $E_{T,lim}$ the tolerance limit of $E_{T,i}$.

The algorithm steps are described in the following:

Step 1: For each state from a set of *n* states of non-compromised IoT device is measured and stored $E_{T,i}$ (i=1,…,n)

Step 2: $E_{T,mean} = \frac{1}{n}\sum_{i=1}^{n} E_{T,i}$ is measured

Step 3: $E_{T,lim} = k \times E_{T,mean}$ is measured

Step 4: After each cycle of the system monitor *t*:

- $E_{T,t}$ is measured and stored;
- If $E_{T,mean} - E_{T,t} > E_{T,lim}$ then declare as compromised the t state (using the energy value of current waveform).

The value of $E_{T,lim}$ is practically chosen equal to $k \times E_{T,mean}$ (Step 3), in order to account for variations of memory usage in various compromised states and possible measurement inaccuracies. Note that this value affects the detectability of compromised IoT devices and it has been chosen heuristically based on previous experience and on the literature [2, 10, 11].

III. Experiment

In order to compare the experimental results with existing similar implementations of systems for identifying various compromised states of IoT devices, the initial data for the memory usage (in percentages) of the IoT device from [4] is used below. For this purpose, screenshots of the figures from [4] for the memory usage of the IoT device are taken using MS Snipping Tool. The screenshots of non-compromised [4, fig. 2] and compromised [4, fig. 3] (as a result of SQL Injection) devices include only the area without the X-axis and the Y-axis.

Then each of the figures is processed using the graphics editor Paint. The purpose of the processing is to obtain a bmp file containing only white and black pixels with a size of 512x112 pixels. The beginning of the coordinate system is located at the bottom left of the image. Processing of the figures includes the following steps:

- Rotate 90°;
- Flip Horizontal;
- Resize;
- Save as...

Fig. 1 shows the main steps of image processing.

Then each of the bmp files is processed by the author's application program written in C. The result of the processing is text file with as many rows as the bmp image contains. The bmp file format includes a header with a description of the structure and size of the image, followed by the pixel values for each row of the image. The bits representing the bitmap pixels are packed in rows. Pixel values for the first row are displayed at the bottom of the image. The output data from the C program is transferred to an Excel spreadsheet. Each row of the spreadsheet contains the number (starting from the X-axis) of white and the number of black pixels in the image. The data is then processed and memory usage index, i.e. the average value (number of white pixels + ½ of the number of black pixels) / number of pixels on the X-axis in the image, see Fig. 1) in relative units is recorded.

After all, the data in each Excel spreadsheet (relative units) is scaled to the percentages of the memory usage of the IoT device, i.e. from the figures in [4] the initial data for conducting the experiment in this paper is obtained in tabular form.

Due to the limited size of the current paper in [7] are given the proposed program written in C and the output files from the processing: bmp and excel files (data is presented graphically and in tabular form) for the memory usage of the IoT device, in the case when the device is non-compromised and in the case when it is compromised.

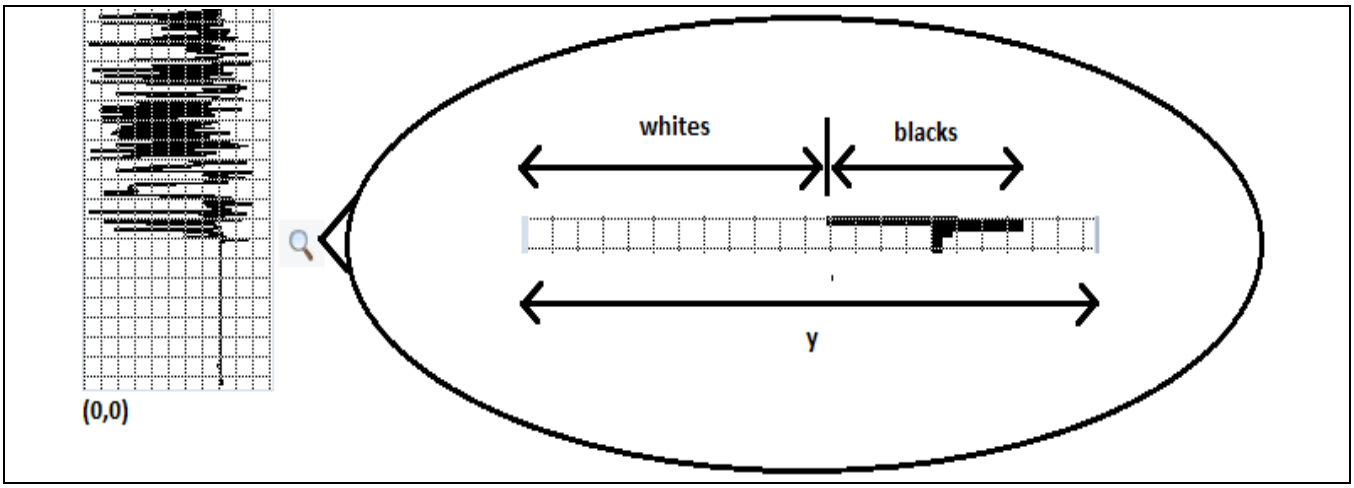

Fig. 1 Image processing in the Paint graphics editor

A Python script [8] has been written by the authors of the paper and the main part is shown in fig. 2. The purpose of the script is to calculate a single value for the trend, T. This is achieved by iteratively calling the function **dwt (x, 'haar')** from the module **pywt** to calculate the coefficients of the trend (for the first, second, ..., eighth level of decomposition), taking into account only the trend coefficients of the previous decomposition level. The while loop stops when a single value for the trend, T is calculated, i.e. there is only one element in the array T, which type is **numpy.ndarray**. The last obtained coefficient for the trend T is squared in order to calculate the energy, E.

```
import os
import platform
import pandas as pd
import pywt

cwd = os.getcwd()
df = pd.read_csv(cwd + "/CSV/mem1.csv")
testValues = df['Value'].to_list()
T , D = pywt.dwt(testValues, 'haar')
while len(T) > 1:
    testValues = T
    T , D = pywt.dwt(testValues, 'haar')
```

Fig. 2. Python script

Results from the Python script execution on memory usage data of the IoT device are shown in table. 1. The first row of the table shows the coefficient of trend, T and the energy, E for the memory usage of a non-compromised IoT device, and in the second line shows the coefficient of trend, T and the energy, E for the memory usage of a compromised IoT device. Also, a third row is added to the table, in which the difference in percentages between the energy E for compromised and non-compromised state of the IoT device is given.

The obtained results for CPU and network interface card usage of a non-compromised and a compromised IoT device are given in table 2 and table 3.

TABLE 1. RESULTS FOR MEMORY USAGE

	T	E
Non-compromised	539.2	290726
Compromised	567.3	321829
ΔE		10.7 %

TABLE 2. RESULTS FOR CPU USAGE

	T	E
Non-compromised	420.3	176652
Compromised	430.5	185330
ΔE		4.91 %

TABLE 3. RESULTS FOR NIC USAGE

	T	E
Non-compromised	231.8	53731
Compromised	227.2	51620
ΔE		-3.93 %

The comparison of the results using the indexes for the memory usage (Table 1), CPU usage (Table 2) and NIC usage (Table 3) shows that the difference between the energy E for a compromised and a non-compromised IoT device is biggest for memory usage ΔE = 10.7%. This corresponds to the results and conclusions from [4], which is also a verification of the obtained results. On the other hand, it is suitable to choose the value of the coefficient k (step 3) to be equal to 0.1, i.e. slightly below ΔE = 10.7% (Table 1) in order to take into account the variations in the memory usage of the IoT device in different compromised conditions and inaccuracies in monitoring.

This paper is sponsored by Scientific and research sector, TU-Sofia,
contract № 212ПД00001-09

IV. Conclusion

An intelligent system for identification of compromised IoT devices due to cyberattack, using Wavelet transformation and Haar filter for the indexes of memory usage has been proposed. The results obtained in the present paper are expected to find application in engineering practice, and can be implemented in the education process at the Technical University of Sofia.

As a further work we plan to study the applicability of the developed model in the cybersecurity of the Internet of Things and identification of compromised IoT devices (as a result of cyberattack) more accurately. Improving accuracy in identification will be based on the methods of the artificial intelligence systems by monitoring the usage of the memory, CPU and network interface card.

The future work includes the following stages:

- Development and implementation of a monitoring system for devices in IoT network keeping in mind that if this would be an intrusive monitoring, it will kill the worst-case execution time.;
- Development of hardware and software implementation of the system for detection of compromised IoT devices as a result of the cyberattack on FPGA;
- Clarification of the parameters of the system for identification of compromised IoT devices as a result of a cyberattack;
- Verification and validation by comparing the results with the results of known models which solve similar problem.

References

[1] Hristov, A, R. Trifonov, An application for temperature monitoring of integrated circuits of bitcoin miners, CAx Technologies Journal, issuue No 7, December 2019, ISSN 1314-9628, pp. 19-24

[2] Hristov, V., REMOTE CONTROL OF DEVICES TROUGH SSH TUNNEL, Bulgarian Journal for Engineering Design, issue 38, January 2019, ISSN 1313-7530, pp.21-26.

[3] R. Trifonov, et. al. Network and Information Security, Avangard Prima, 2013, ISSN 978-619-160-183-7 (in Bulgarian).

[4] Sukhoparov M. E., Lebedev I. S. Identification the Information Security Status for the Internet of Things Devices in Information and Telecommunication Systems. Systems of Control, Communication and Security, 2020, no. 3, pp. 252-268 (in Russian.

[5] Tan L., J. Jiang. Digital Signal Processing 2nd Edition, Academic Press, ISBN: 9780124158931, 2013.

[6] Zendara O., et. al. Swarm intelligence-based algorithms within IoT-based systems: A review

[7] https://github.com/sashkinaaa/readValuesFromBMP

[8] https://github.com/sashkinaaa/Haar_1D_Filter/blob/main/pywt-haar1D.ipynb.

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6308658/

[11] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot