METHODOLOGY FOR EVALUATING IOT SECURITY BASED ON DEVICES BEHAVIOR

Catalin BOJA
Bucharest University of Economic Studies, Romania
catalin.boja@ie.ase.ro

Abstract: *IoT devices are becoming more and more present in our life as they are starting to automate business and personal life routines. Despite their real advantages, we confront to an almost non-standardized environment that contains a wide range of different devices from multiple manufacturers, devices that provide different capabilities. This creates the premises for a complex environment that needs to be secure. The paper proposes a methodology for evaluating IoT devices security based on a set of criteria that focuses on their behavior. In this way the methodology provides a security evaluation framework that is independent of the device hardware and software characteristics.*

Keywords: IoT, security, methodology
JEL classification: L86
DOI: 10.24818/ie2020.01.08

1. Introduction

Today IoT devices are not just the simple, “dumb”, sensors that record a value from environment in which they operate and send it to a local network collector device or service. They can connect over Internet to different services, to do complex monitoring of an event, to respond to remote commands and even to implement autonomous behavior. Even if they are designed for a single task, they have the computing power and the software architecture that can allow attackers to install additional routines and reconfigure them at runtime to do other things. One of the recent biggest Distributed Denial of Service (DDoS) attack has been conducted by exploiting a large army of IoT devices, which were infected by the Mirai malware [1]. The malware was able to infect a wide range of Internet connected devices, like routers CCTV cameras, Web cameras, printers, and make them flood with requests different IP’s, which were targeted by the attackers.

To provide a richer user experience for end users, especially home users, developers and manufactures are offering a wide range of home or personal IoT devices that are connected to Internet by different communications channels, are controllable remotely by Internet service and are implementing or not different cybersecurity protections measures. This creates a complex scenario in which vulnerabilities can be easily found and exploited by an attacker.

In this dynamic environment, with so many layers and components, is quite a challenge to provide full security. There are so many characteristics that must be secured and there is a large community of hardware manufacturers and software developers who approach the security perspective of their products from different perspectives, which in most cases are not regulated. Previous research results, [5-8], shows the complexity of the field, not because of the cryptographic and cybersecurity solutions that can be used, but because of the different ways those solutions are or not implemented and the wide range of IoT devices and services.

The IoT security perspective provided by this paper focuses on the common characteristic of all attacks on IoT devices, which will make them behave differently or strange from different perspectives. This research focuses on providing a security evaluation for different IoT devices by monitoring their behavior and flagging events which are out of the range of a normal behavior. The proposed methodology can be used to analyze if an IoT device represents a security risk. It cannot be used to protect an IoT device, but it could be used to detect a hacked or compromised device in the early stages of a successful attack.

2. Evaluation criteria

A general IoT device architecture is defined by three layers, including perception layer, network layer, and application layer. This is the general architecture which other studies have considered when assessing the IoT Security of a device [1][2]. If we extend it to include the service provider, then the architecture will have components which are not on premise, but in Cloud [3][4], as in Figure 1. In terms of security, the new layer exposes specific security risks which must be addresses both on the Internet communication channel and at the service provider [4].

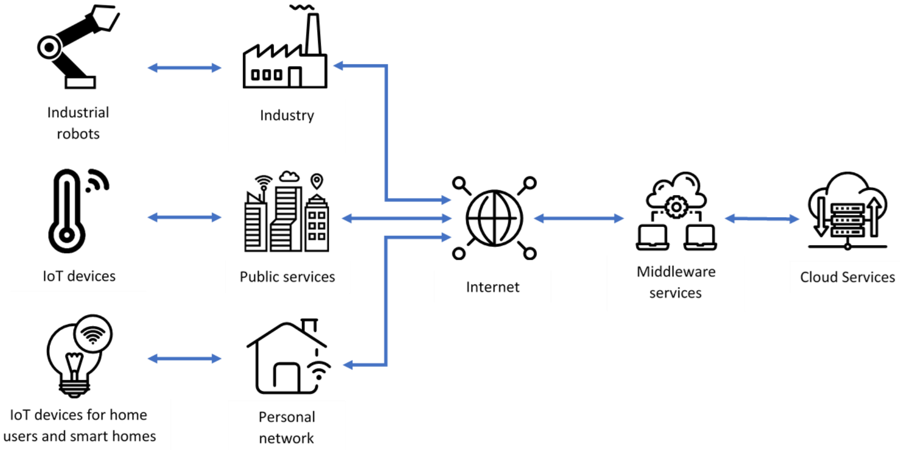

Figure 1. General IoT Architecture contained both devices and services. Source: own. Icons from flaticon.com

The proposed methodology is focused on analyzing the IoT device behavior based on the Network layer. This approach is independent of the software and hardware characteristics of different IoT devices and it allows us to do a black-box evaluation. The methodology can be applied on any IoT devices that are using a communication channel to send or receive data. Also, the methodology addresses especially devices that are using IP connections and by that are vulnerable to remote attacks from Internet.

IoT devices that are using RFID, Zigbee, Z-Wave, Bluetooth or Bluetooth Low Energy (BLE) are vulnerable from local or proximity attacks and they operate behind a gateway which should provide its own layer of security. Monitoring Zigbee, Z-Wave and Bluetooth environments requires specialized equipment which limits the applicability of this methodology [2]. Nevertheless, from the gateway perspective, the methodology can provide an internal security module that can evaluate the state of the local network or of the connected devices:

- Denial of Service attacks on Z-Wave and Bluetooth devices or on their gateway will generate a spike in bandwidth and packets frequency.
- Replay attacks will trigger an increase traffic in valid packets.

From the wide range of security characteristics that can measured for an IoT device, [9] [10], the proposed methodology includes:

Bandwidth – devices that use high bandwidth represent a bigger security risk because it is more difficult to filter normal traffic from abnormal one, generated by a compromised device. It is more difficult to detect a security issue in verbose systems that generate a lot of traffic as the attacker can hide in that.

Transmission frequency – most IoT devices provide a pattern for transmitting data as they are configured to send regular updates at specific intervals. Passive IoT devices that monitor temperature, power consumption or other environment characteristics will send recorded data based on its configuration settings. The transmission frequency can be easily used to define a device behavior fingerprint and any changes will be easily detected. Based on this methodology, devices with well-defined transmission frequency will provide a better security level.

Packets size – as software is a deterministic environment, each protocol or software solution is characterized by predefined network packets in terms of structure and size. This allows clients to communicate with end points, so each party will be able to read and interpret the received packet. Each protocol, public or proprietary, has a packet size and by knowing that information we can determine if a device is showing a change in this behavior in time. By packet size we consider a complete get, update or put request. For example, a smart thermometer will connect to the gateway and send the recorded temperature.

Protocols – there are taken into consideration the protocols used by the device to communicate with the gateway or other services. From this perspective, there are protocols that implements security by design, as HTPPS, or do not provide security.

Local ports – we analyze if the device is listening on standard or non-standard ports. This is sometimes a common practice of the manufacturer to allow service backdoors that will be used to push updates or to collect status and usage statistics. From security perspective this is a major issue as these details are less documented and end users have no idea on how these services are protected. In this methodology, these problems are classified as major security risks.

Destination IPs – we separate the destination IPs in local and public Internet addresses. This perspective analyzes and defines a collection of local and public IPs to which the device will initiate connections. Devices that connect to public IPs are more vulnerable to sniffing attacks and can reveal personal data if the connection is not encrypted, as anyone that has access to it can implicitly read the data. Also, connecting to local IPs over Wi-Fi exposes the same problem as the Wi-Fi environment is an open environment and anyone close enough can capture the packets. The major difference between Internet connections and local Wi-Fi connections is given by the exposure. Over Internet you are exposed to anyone, but for Wi-Fi we could say the attack must be local, as the attacker should be in the proximity of the Wi-Fi router.

Table 1. Behavior based evaluation criteria from security perspective

Criteria	Measure unit	Low Security	High Security	Optimum
Bandwidth	Mbits in 1-hour interval (Mbph)	High volumes of data	Low volumes of data	< 1Mbph
Transmission frequency	Packets per hour (Pph)	High frequency	Low frequency	1 Pph
Packets size	Kbits	Big packets. Nonstandard ones	Small packets. Standard structure	1Kb
Protocols	Number of protocols	Nonstandard or unsecure protocols	Standard secure protocols	1 secure protocol

Local ports	Number of local ports	Device listening on any number of local ports	No local ports exposed	0 ports
Destination IPs	Number of destination IPs	Many Internet public IPs	No public IPs. Only local IPs if needed	1 local IP

Table 1 provides a summary of the evaluation criteria and gives a short description of different security perspectives, from low to high and from an optimal value. The proposed optimal value describes a “perfect” scenario in which devices are sending minimum amounts of data and have a very low footprint on network. This optimal profile is difficult to achieve but the proposed methodology is assessing the device security risk from this ideal perspective. As devices profiles are moving away from those values, they will expose more data on the network and will provide a more vulnerable profile.

3. Evaluation strategy

The proposed methodology consists of applying a four-stage process that will allow anyone to analyze an existing IoT device and place it in a security risk category based on its behavior. The values for the considered evaluation criteria can be obtained by analyzing and measuring the network traffic generated by the device. This can be done automatically using a local proxy or by manually motoring the traffic using WireShark. The evaluation is done in the local intranet gateway or in a proxy to which the gateway connects to get access to the Internet, as in Figure 2.

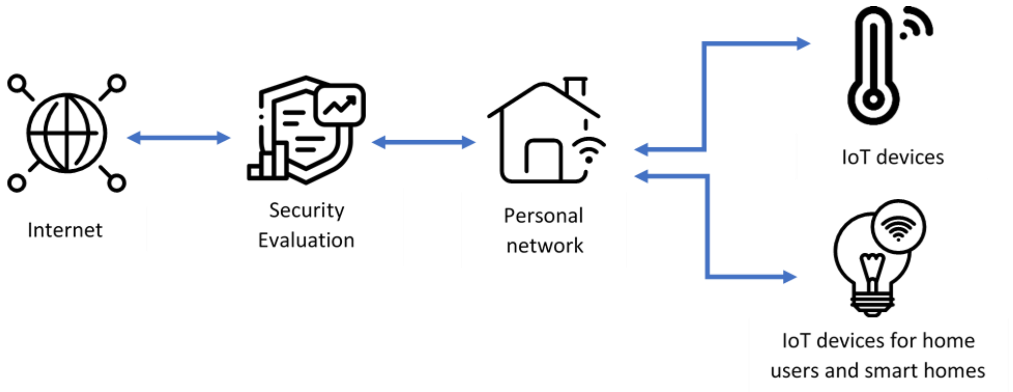

Figure 2. IoT Evaluation Architecture. Source: own. Icons from flaticon.com

Initialization phase is the first stage the is focused on preparing the evaluation environment. A general evaluation framework, as the one in Figure 2, is prepared by routing the entire IoT environment traffic through a central gateway or a proxy.

Monitoring phase is the second stage of the evaluation methodology in which we record data that should describe the normal behavior pattern of the IoT device. In this stage it is important to run the IoT devices in their initial state, out of the box or after a hardware reset. The initial configuration and the power on cycle of most IoT devices will trigger update or other internal routines. The evaluation module will record the data associated with the previous evaluation criteria. The stage can last from several minutes until we are sure that we cover all functions that the device allows.

Profile set phase is the third stage of the evaluation methodology and it has the objective to define the IoT device profile based on final values of the evaluation criteria. The profile consists in a datasheet that gives us the values that describes the device network behavior. For characteristics that give variable values during the monitoring stage, like used bandwidth and packets number, the methodology considers an average value.

Security risks evaluation is the final stage of the methodology and has the objective to produce the security evaluation of the IoT device by classifying it in a risk group.

The methodology computes the distance of the evaluated IoT profile from the ideal one. Greater the value, greater the security risks that characterizes the IoT device.

Table 2. Classification scale for evaluated criteria

Criteria	Optimum	0 points	1 point	2 points	3 points
Bandwidth	1Mbph	<= 1 Mbph	< 10 Mbph	< 100 Mbph	Up to 1 Gbph or more
Transmission frequency	1 Pph	1 Pbh	< 10 Pbh	< 100 Pbh	>= 100 Pbh
Packets size	1Kb	<= 1Kbph	< 100 Kbps	< 1 Mbps	>= 1 Mbps
Protocols	1 secure protocol	For 1 secure protocol	For each additional secure protocol	For each unsecure protocol	

For criteria that can give big differences between recorded values and optimal one, the methodology uses a classification scale, as in Table 2.

Using the proposed methodology, the IoT device profile is translated in a value that varies between 1, when the device send minimum amount of data and connects to a single local IP using a secure protocol, and a value greater than that.

4. Conclusions

As research has shown, [11-12], the IoT field is a very dynamic one and is constantly growing by including a wide range of devices, with different communication and processing capabilities, that connect to a wide range of local and public services. As it is almost impossible to regulate the software and hardware development of these devices, each will be unique as it will have set of security risks and vulnerabilities. Doing a detailed security evaluation of these devices, prior to release to market, is constrained by a lot of factors, including production budgets, team experience, therefor a lot of IoT devices will be delivered to home users with unknown vulnerabilities. As this is a common scenario, one defense will be to evaluate the risk of used IoT devices and monitor them during their usage. Using the proposed methodology, we can have a degree of understanding the security risks of different IoT devices based on something that they all have in common, network behavior, and something we can measure externally. This approach can also be used to detect if an IoT device will change its normal behavior and that could be the trigger for a deeper analysis of a possible compromise device.

Acknowledgment

This paper presents results obtained within the PN-III-P1-1.2-PCCDI-2017-0272 ATLAS project ("Hub inovativ pentru tehnologii avansate de securitate cibernetică / Innovative Hub for Advanced Cyber Security Technologies "), financed by UEFISCDI through the PN III – "Dezvoltarea sistemului national de cercetare-dezvoltare", PN-III-P1-1.2-PCCDI-2017-1 program.

References

[1] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," 2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, 2017, pp. 6-12, doi: 10.1109/ICSSA.2017.12.

[2] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, "SoK: Security Evaluation of Home-Based IoT Deployments," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 1362-1380, doi: 10.1109/SP.2019.00013.

[3] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 663-667, doi: 10.1109/CIS.2013.145.

[4] C. Toma, A. Alexandru, M. Popa, A. Zamfiroiu, “IoT Solution for Smart Cities’ Pollution Monitoring and the Security Challenges”, Sensors 2019, 19, 3401.

[5] W. Leister, M. Hamdi, H. Abie, S. Poslad, A. Torjusen. “An Evaluation Framework for Adaptive Security for the IoT in eHealth”, International Journal on Advances in Security, vol 7 no 3 & 4, year 2014, http://www.iariajournals.org/security/

[6] L. S. Medeiros, F. Zuvanov, F. L. de Mello, E. Strauss, “IoT Information Security Evaluation for Developers and Users”, Journal of Information Security and Cryptography (Enigma), Vol 4, No 1 (2017), https://doi.org/10.17648/enigma.v4i1.63

[7] Sajjad, Hamza & Arshad, M. (2019). Evaluating Security Threats for each Layers of IoT System. Volume 10. 20-28.

[8] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, thirdquarter 2019, doi: 10.1109/COMST.2019.2910750.

[9] Common Criteria, “Common Methodology for Information Technology Security Evaluation”, Evaluation methodology April 2017, Version 3.1, Revision 5, CCMB-2017-04-004, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

[10] Microsoft, “Evaluating Your IoT Security”, whitepaper, https://azure.microsoft.com/en-us/overview/iot/?site=mscom_iot , 2017

[11] Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. Information 2016, 7, 44.

[12] S. A. Kumar, T. Vealey and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 5772-5781, doi: 10.1109/HICSS.2016.714.