DOI: 10.53477/2668-2001-21-36

INTERNET OF THINGS SECURITY FRAMEWORK

Dorin Iordache[1]
"Ovidius" University

Abstract

It was unimaginable for a non-professional user that access data to personal e-mail, bank or identity accounts could be stolen via a mobile phone interface or connection, no more than twenty years ago. Nowadays, people with bad intentions – hacker – can use smart devices, such as: webcams, microwaves, refrigerators, door controllers, and others, generically we named it IoT[2], to access accounts like the ones mentioned above, without much effort. The Internet of Things is the place where devices are digitally interconnected, interacts with almost every domain. IoT development is closely correlated with growing of Internet. These issues have generated an unprecedented upward trend in Wi-Fi and IoT interconnecting networks. Cyber-security has gained new meanings because of the increasing number and scope of IoT devices. By developing these devices, especially among regular users, it is necessary to improve their security more than ever. How prepared are regular users and how can they protect themselves in the context of IoT penetration into their daily lives? it is a question that needs to be answered, in terms of the actions it can take immediately or in the long run.

Keywords: IoT; cybersecurity; Wi-Fi access point; network interface.

INTRODUCTION

By the Internet of Things (IoT), as terminology, we understand a multitude of things, objects for a lot of people interconnected via the global Internet network.

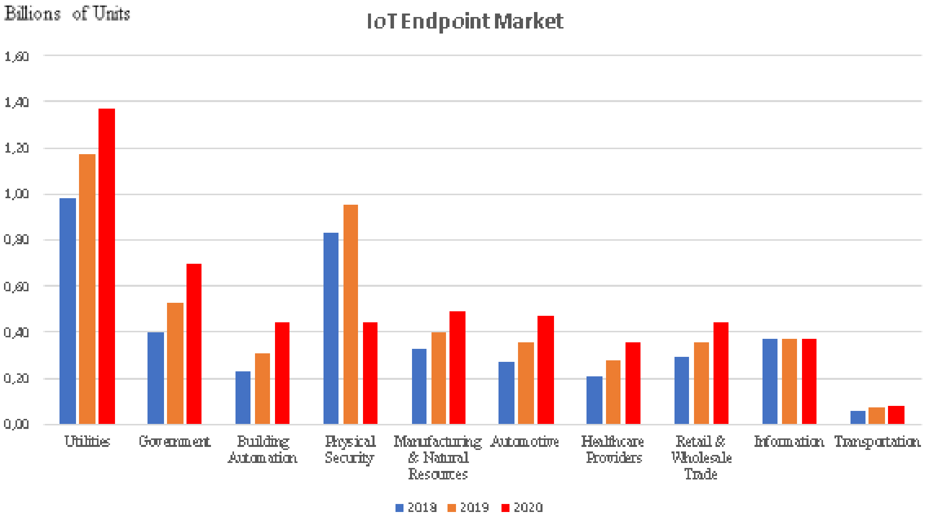

Figure 1. IoT Endpoint Market 2018-2020[3]

For the ordinary or professional user, it can be about: TV, webcam, intelligent central heating, or air conditioning thermostat, all interconnected. The IoT term is known for a long time if we refer to certain components of industrial robotics.

[1] Corresponding author: dorin.iordache@365.univ-ovidius.ro
[2] IoT - Internet of Things
[3] EGHAM. 2019.

IoT devices are found in operational environments and in the daily life of ordinary users, but also industrial users: connected cars – embedded (consumer and commercial), outdoor surveillance cameras, doors control, small smart weather stations, etc., as shown in Figure 1.

What is new and in an exponential development is represented by the entry into personal use, at home, on the one hand, and the functioning independently of human action, on the other hand. (EGHAM 2019.)

The trend in the coming years for the IoT field is of constant growing, even explosive, both in terms of the number of devices as well as in the field of use. According to STATISTA, $ 749 billion is estimated to be spent on the Internet of Things (IoT). Even if in 2021 there will be a reduction in the costs, due to the COVID 19 pandemic, by 2023 an amount of $ 1.1 trillion is estimated for IoT. As a result, IoT security is becoming increasingly important, with significant amounts allocated to the field. Thus, more than $ 120 billion were spent on IoT security in 2019 worldwide. (STATISTA 2021.)

The data from these IoT sensors and controllers are extremely valuable for changing user and business behaviors. Using data for better business decision making and automation for better efficiency is extremely valuable - and the basis for business moves, as advertising was Industry 4.0.

Thus, according to some estimates, with the increase in the number of IoT devices, the need for the communications bandwidth will increase also. The current trend is to use 5G technology. As shown in Figure 2, if in 2020, 70% of all IoT devices were owned by outdoor surveillance cameras, while connected cars- embedded were only 11%, in 2023 the ratio will change in favor of the latter, with an index increase by about 400%, while the number of outdoor surveillance cameras will be reduced by 50% as a share of total IoT devices in correlation with the 5G technology. (Alan Weissberger 2019.)

With the increase in the number and diversity of areas of use of IoT devices, new possibilities open up for hackers who will exploit their vulnerabilities.

Some of their vulnerabilities have brought IoT security into the multitude of cyber security issues that need to be addressed quickly enough.

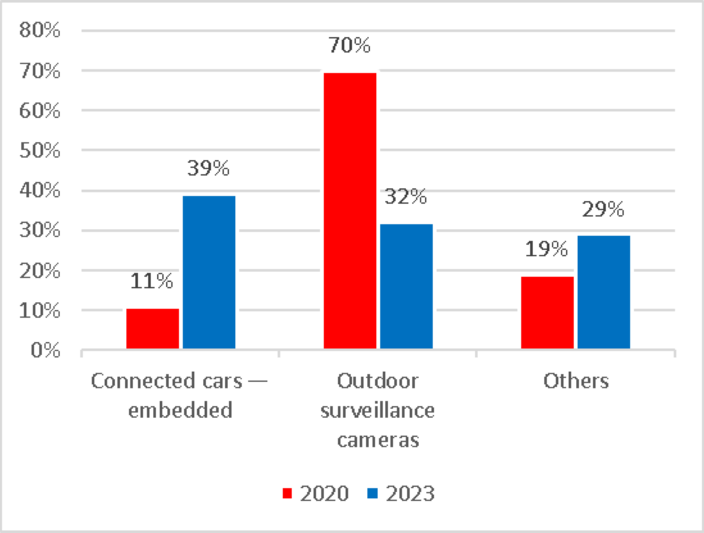

Figure 2. 5G IoT Endpoint Installed Base, Worldwide[4]

IOT DEVICES SECURITY

IoT security is the technological area involved in protecting devices and networks connected to the Internet of Things (IoT). IoT involves adding Internet connectivity to a system of interconnected computing devices, mechanical and digital machines, objects and/or people. The growth of the IoT devices market in Europe, reaching over 242 billion Euros[5], will have as affect the development of IoT

[4] Alan Weissberger, 2019

[5] https://www.peerbits.com/blog/biggest-iot-security-challenges.html

applications that will implicitly generate new and multiple cyber security challenges. Because the manufacturers of these devices compete to provide users with the latest and most handy smart device, few of them are really concerned about the security issues associated with accessing and managing personal data, but also with the intrinsic security of the IoT device itself.

Therefore, it is important to know what the important common security challenges are affecting IoT devices.

Current IoT security challenges

According to the Symantec Internet Security Threat Report study (Symantec 2018. vol.23) the most important challenges can be summarized in:

- Insufficient software testing and updating of IoT devices, both in the manufacturing process and especially in the end-user operation process[6];
- Vulnerable to brute-force attacks targeting the exploitation of default passwords[7];
- Malware and ransomware attacks that use IoT devices as a means of penetrating computer systems[8];
- Botnet targeting cryptocurrencies, with an explosion of use, especially in the last pandemic year[9] [10] (Jeremi Kirk 2020.)
- Data security and privacy (mobile, web, cloud (ISO 2005.)
- Attacks on data security and privacy;
- Use and exploitation of elements of artificial intelligence;
- Remote access to resources within the network architecture through the IoT devices[11] [12];
- all these actions are often illegitimate and have an illicit purpose.

IoT vulnerabilities

The OWASP – Internet of Things Project (OWASP 2018.) is designed to help manufacturers, developers, and regular users to better understand the security issues associated with the Internet of Things. The project allows users who act in any context to make the best security decisions when building, implementing, or evaluating IoT technologies. The project aims to define structures for various sub-projects that may or may not include IoT devices.

Within this project, in 2018 the 10 most important aspects regarding IoT security were published: (OWASP Top 10. 2018.)

- Weak passwords (Ant Allan.2020.);
- Unsecured network services;
- Systems that have unsecured interfaces;
- Lack of a secure update mechanism;
- Use of unsecure or technologically obsolete components;
- Insufficient protection of privacy;
- Unsecured data transfer and storage;
- Lack or insufficient management of devices;
- Unchanged or known default settings;
- Lack of security to physical attacks;

[6] American Consumer Institute Center for Citizen Research

[7] https://www.varonis.com/blog/the-mirai-botnet-attack-and-revenge-of-the-internet-of-things/

[8] https://bdtechtalks.com/2016/08/22/the-iot-ransomware-threat-is-more-serious-than-you-think/

[9] https://www.globenewswire.com/news-release/2020/03/11/1998560/0/en/February-2020-s-Most-Wanted-Malware-Increase-in-Exploits-Spreading-the-Mirai-Botnet-to-IoT-Devices.html

[10] https://unit42.paloaltonetworks.com/los-zetas-from-eleethub-botnet/

[11] https://arstechnica.com/information-technology/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/

[12] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

VULNERABLE IOT INTERFACES AND SERVICES

Based on security challenges and IoT vulnerabilities, the risks, vulnerabilities of IoT devices present in the user's ecosystem can be defined, as well as the way of performing possible attacks, with the aim of counteracting these attacks or reducing residual risk, where these devices exist.

Once the most important risks and vulnerabilities of IoT devices in the study ecosystem have been identified, a possible scenario can be generated regarding the execution of possible attacks, of a malicious person (hacker), who acts for various purposes, most of the time illegitimate.

Mainly, the action of an attacker can be summed up in actions aimed at altering one or more components concerning confidentiality, integrity, and availability of information, managed within IoT devices, or within the ecosystem in which they are present.

Based on the above, the main interfaces and services through which an attacker can exploit them, we have identified the following:

Web services and interfaces

Through web services and interfaces, attackers exploit vulnerabilities in principle to:

- identify equipment access information: type, software version, firmware version, data about access accounts: username and passwords (whether or not they are the default ones);
- identify active / open web service ports;
- access information regarding the interaction with web services, through the administration interface, to alter the configuration, redirect certain services and/or intercept and record data traffic.

Local area network interfaces

Having as main purposes:

- identification of the network configuration, both hardware and software;
- the installation of malicious programs in the systems of the local network;
- changing the local network configuration (network addresses, routing tables, etc.);
- theft or destruction of data processed in the component systems, used for various purposes, including extortion;
- monitoring the network activity in order to further exploit the identified vulnerabilities.

Wireless network interfaces

Are most often exploited for the purpose of:

- identifying the network configuration;
- identifying the existing open services and ports;
- interception and recording of data traffic;
- identifying the network access data, adding of new privileged accounts, as well as executing harmful processes, for further exploitation.

These elements will be used to define a minimum framework of measures required to be performed by a regular user, with the aim of reducing the risks and vulnerabilities of current IoT devices encountered in a personal ecosystem, while maintaining an acceptable level of security

UNPROFESSIONAL USER DIRECT ACTIONS

In the current context, because IoT devices are developing almost exponentially and are widely present in the lives of ordinary users - non-professionals, usually without computer or cyber security knowledge, it is necessary to provide them with sets of simple organizational and technical measures, by which an acceptable level of risk can be maintained.

Following the analysis of the information contained in the generated reports, based on the main types of IoT devices and their most current risks, represented in figures 3 and 4, we can conclude the following:

- over 46,000 IoT devices have default authentication data[13];
- over 80% of these devices use the HTTP / HTTPS protocol or allow a telnet connection;
- over 80% of webcams use HTTP protocols, with different ports open[14].

This information, corroborated with others obtained using OSINT[15] technologies, represents important ways and means of exploitation and use of penetration techniques for an attacker. At the same time, it is important information for the community of security administrators, to fight possible attacks on IoT ecosystems.

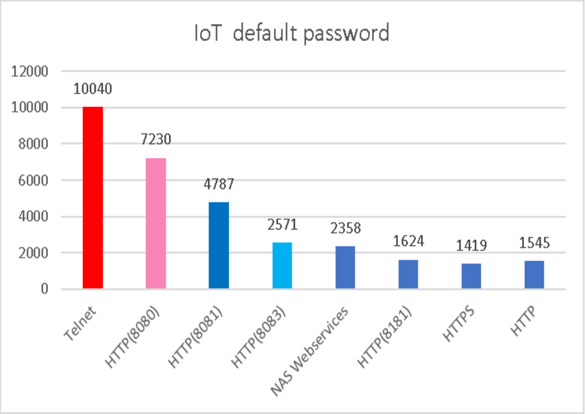

Figure 3. IoT devices with the default password

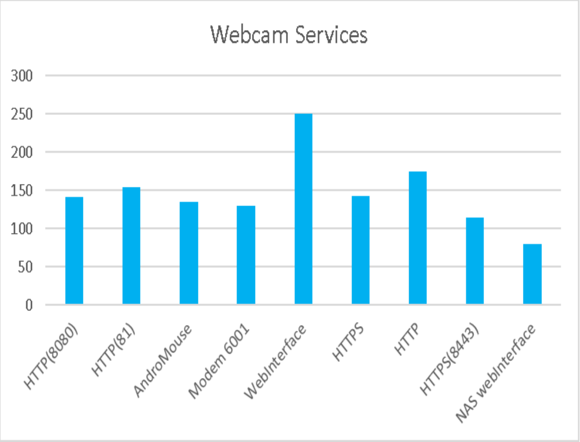

Figure 4. Webcam available sevices

On the other hand, we find the need to provide non-professional users with simple, basic knowledge and procedures, with which they can manage their security risks at an acceptable level, because of using IoT devices.

These actions can be categorized into:

- organizational actions, comprising a minimum set of guides / guidelines, and
- technical actions, which consist in the execution of simple, predefined or minimally configurable commands, through which the user identifies architectural elements of his own network ecosystem.

Managed actions

We propose to the user to read at least the main elements of access to IoT devices, specified in the technical documentation received when purchasing them.

We also propose to the user the completion of the synoptic for each device, specified in table 1, as follows:

Table 1. User action checkmark

No.	Action	How-to	Check	Notes
1	Read documentation	Read the documentation and find the information about the access for the admin interface	Yes/No	
2	Access to admin console	Access the management console using the information in section 1	Yes/No	
3	View default configuration	Write in the table 2 the information found: device name, IP address, firmware version, MAC, manufacturer.	Yes/No	
4	Change default access account information	Change at least the administrator account access password.	Yes/No	admin; administrator; root;

[13] https://www.shodan.io/report/CloKjAm0
[14] https://www.shodan.io/report/MwhZCMPZ
[15] OSINT - Open-Source Investigation Tools

No.	Action	How-to	Check	Notes
5	Password complexity	Set a strong password: it must be at least 10-13 characters long and contain at least one uppercase, numeric and special characters.	Yes/No	Do not test the strength of your password using any specific websites.
6	Memorize the password	Remember the password. Do not write it on any medium. Do not tell anyone.	Yes/No	

Technical actions

The handiest actions available to the non-professional user refer to the identification of the network architecture and IoT devices present in his own ecosystem. We propose that the completion of information to be managed according to the structure presented in table 2. One table entry will be completed for each device.

The information can be found, either by referring to the technical documentation or by running simple programs, usually freeware.

Table 2. IoT configuration matrix

No.	IoT device	IP address	Port	Services	OS[16]	MAC	HOP number	Producer	Firmware version
1	TV	192.168.100.27	80, 443, 9090	HTTP, ssl, X11, upnp	Linux 2.6	6 digits goups	n	Manufacturer	123456
-	-	-	-	-	-	-	-	-	-

To identify the architecture, we tested freeware utilities, through which a user without knowledge in the field of computer networks is more difficult to achieve. Freeware software products capable of scanning your own network ecosystem can be used using the nmap[17] utility.

Following the execution of the program, the network architecture, and the "*targets*" to be analyzed are identified, and then we will select the network analysis profile.

We have reproduced some of them below, considering that we will analyze the address 192.168.100.1:

- intense scan: *nmap -T4 -A -v 192.168.100.1*;
- Intense scan plus UDP: *nmap -sS -sU -T4 -A -v 192.168.100.1;*
- Intense scan, all TCP ports: *nmap -p 1-65535 -T4 -A -v 192.168.100.1;*
- Quick traceroute: *nmap -sn --traceroute 192.168.100.1.*

The address 192.168.100.1 will be replaced with the address in your own network.

Following the execution of these commands, the information necessary to complete the data in the model specified in table 2 will be searched and identified.

By periodically executing such commands, the user can identify any configuration changes, by comparing them with the reference data recorded in the two tables.

CONCLUSIONS

With the broadening of the number and areas of use of IoT devices, the degree of insecurity has increased. Personal data and private life are even more imperative to be protected. This can be done by specially trained staff, those specialists in cyber security, involving the spending of sums of money. Therefore, this activity must be able to be carried out, even if limited, by the common, ordinary user, the non-professional one, because it does not involve financial expenses.

At the level of an organization (ISO/IEC 27001) there are sufficient material, technical, human, and financial resources to implement operational standards specific to the field of cyber security (Mona Mangat. 2020.). At the level of the individual, non-professional user, there are certain difficulties in implementing cyber security measures, because the resources available are limited and insufficient.

[16] OS - Operating System
[17] https://nmap.org/zenmap/

Therefore, we identified and proposed two major actions: organizational actions, focused mainly on the minimum education of the non-professional user, but also by providing a simple organizational framework consisting of two models to complete specific data, and indicating a freeware tool, easy to use and understand, because the user will be able to identify the data to be stored in the two models in the information on the screen display of the execution of those commands.

We intend, in the next stage, to validate by running a survey on the use of the risk reduction framework and on reducing the security vulnerabilities of IoT devices, addressed to target users, i.e. non-professionals in the IT field.

REFERENCES

Ant, Allan. 2020. “Best Practices for Managing Passwords: Policies Must Balance Risk, Compliance and Usability Needs”, https://www.gartner.com/en/documents/1401917/best-practices-for-managing-passwords-policies-must-bala. Accessed December 10, 2020.

Weissberger, Alan. 2019. “Gartner: 5G IoT endpoints to triple between 2020 and 2021”; Surveillance cameras to be largest market over next 3 years, October 17, 2019, https://techblog.comsoc.org/2019/10/17/gartner-5g-iot-endpoints-to-triple-between-2020-and-2021-surveillance-cameras-to-be-largest-market-over-next-3-years/

EGHAM. 2019. “Analysts to Explore How IoT Will Accelerate Digital Transformation Initiatives at the Gartner IT Symposium/Xpo”, Gartner study 2019, November 3-7, 2019 Barcelona, Spain, https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

ISO. 2005. “ISO. Security techniques { code of practice for information security management”, 2005.

ISO/IEC 27001. “INFORMATION SECURITY MANAGEMENT”, https://www.iso.org/isoiec-27001-information-security.html

Kirk, Jeremi. 2020. “Heh' Botnet Targets Telnet on IoT Devices”, https://www.bankinfosecurity.com/heh-botnet-targets-telnet-on-iot-devices-a-15127. Accesed December 10, 2020

Mangat, Mona. 2020. “19 Cybersecurity Best Practices to Protect Your Business”, March 9, 2020, https://phoenixnap.com/blog/cybersecurity-best-practices. Accessed January 10, 2021.

OWASP. 2018. “Internet of Things Project OWASP” https://wiki.owasp.org/index.php/OWASP_ Internet_ of_Things_Project, 2018. Accessed May 10, 2020.

OWASP Top 10. 2018. “Top 10 Internet of Things OWASP”, https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf, 2018. Accessed March 10, 2020.

STATISTA. 2021. “Statista Research Department, Internet of Things (IoT) spending worldwide 2023”, Jan 14, 2021, https://www.statista.com/statistics/668996/worldwide-expenditures-for-the-internet-of-things/

Symantec, 2018. vol.23. “Symantec Internet Security Threat Report”. ISTR Vol. 23, 2018, Last access January 10,2021 https://docs.broadcom.com/doc/istr-23-2018-executive-summary-en-aa