ISSN 2587-1943

SMART SECURITY OF IOT AGAINST DDOS ATTACKS

Ahmet Efe 1, Esra Aksöz 2, Neslihan Hanecioğlu 3, Şeyma Nur Yalman 4

Original scientific paper

Since the internet, which is pervasive in every area of our lives, is so inevitable that the number of intelligent systems and devices, which are interconnected, have increased day by day through e-government, industry 4.0 and smart city applications. These devices have led to the emergence of the 'Internet of Things' (IoT) concept to the extent that intelligent systems became widespread. In addition to facilitating the life and functionality of these devices, we also need to take some safety precautions to prevent failures, difficulties and denial of service. In order to take the necessary precautions, we need to know functionality and capability of devices and risks, vulnerabilities and threats as well. We have conducted a survey on taking all kinds of security precautions against DDoS attacks, to contribute to increase the security level of these intelligent devices.

Keywords: *Internet of Things, intelligent systems, E-government, Security of IoT.*

1 Introduction

The keywords start with 'smart' are very popular in nowadays like smart cities, smart watches, etc. All of them are related with Internet of Thing (IoT) technology. Communication of these devices provided via the internet. Also, intelligent transportation will access a web of interconnected data from GPS location to weather and traffic updates via the internet. Also, the traffic lights will light up according to the intensity of the road through the data they get from the internet. These situations will make human life much easier. But these will bring security problems. Because of these operations, a very large amount of data will be generated, and these data will need to be protected. If there is an illegal access to information and attacks in the system of the smart house, it will cause physical disruptions. Because of these situations, all data in IoT need to be protected.

While traditional ransom software enters computers and encrypts files, IoT ransom software can take control of systems used in the real world. Many of the practical advantages of IOT technology are ransom operators who use their own advantage, can cut off electricity, stop vehicles, and even prevent production lines from functioning. These methods, which are much more likely to create more damage, will also increase the amount of ransom money that attackers are willing to give back to their IoT device. If there is a place where such extra ransom could be obtained, the attackers will not be idle.

Some experts think that such an attack can be solved by simply resetting the IoT device, turning it on and off, or starting it all over again. But IoT is not the irreversible effect of traditional ransom software, which makes ransom attacks terrible. This time the dangerous situation is the timing of the attack. Many complex IOT schemes are already in use, which can lead to catastrophic failure to reach critical systems for even a second.

As IoT is increasingly integrated into more critical systems, the inability to reuse the locked systems in time can cause serious harm to the individual and the public. Examples of these critical systems are cardiac pacemakers to power plants. How long do you wait to pay when a relative or your heart rate is disabled by ransom software?

Let's give another example. When intelligent vehicles become widespread, locking only 3 for a short time is enough to overturn the traffic of an entire city. Even worse: think that the subway signaling system does not work for just 1 minute. How many lives get in danger?

Examples of IoT repatriation attacks are also shown. Pen Test Partners, a UK based company, for example, took a smart thermostat with ransom software and ran the thermostat at full power as long as the required money was not paid. This, of course, was just a test. Later, other security companies and software groups, smart homes, intelligent offices, connected and autonomous devices showed how worn-out smart devices could be captured by ransom software.

All elements that make up smart cities, from traffic lights to bus stops or even roads, need to be defended against the pirates because they are interconnected. Developed cyber security methods complicate the work of hackers, but those who manage smart cities should always be on the alert. In this article, we will talk about what we need to do to ensure that the software that forms smart cities is not hacked by data thieves.

IoT security must be cleared from the beginning in the face of all these "demonstrations". In the past few weeks, DDoS attacks were made with 145 thousand IOT compatible cameras (web cameras, security cameras, etc.) captured by cyber hijackers.

2 Problems with IoT in general

There are many risks and threats arising from IoT vulnerabilities. As a simple example can be given from printers that have IoT capabilities. Recently, as seen in the attack on the DNS provider Dyn, probably IoT (objects of the Internet) powered by using botnet DDoS attacks will keep on happening in 2017. by 2016, all an IOT botnet (Mirai) by targeting the Internet one of the big DNS server can be interrupted for hours.

In this case in the hands of almost any person who is the most powerful government actors are prepared for a worldwide communications network. The only way the growth of the phenomenon of IOT botnet security issue being considered to have produced a lot of devices. Patch is written in millions of existing sensitive IOT device, but the patch process was so complex that users prefer to skip the process of patch.

Printer devices found in every office may seem innocent and innocuous at first. However, the writers form one of the most important networks in the office. There is extensive networking between printers and computers in intensive offices, and this poses a high risk for cyber-attacks. Efficient document processing and superior security are now more important to every office. This situation will require more stringent measures, especially in the era of the Internet of Things (IOT).

IoT technologies, which have come to our minds frequently in recent times, are taking place in different areas of our lives day by day. IOT networks can create a variety of usability by connecting many devices at home and in offices. But these technologies and devices add to the business life, as well as threats to data security. Unless security precautions are taken regarding the use of connected devices over the Internet, the possibility of infiltration of important data out of the office is increasing.

Connected devices that do not have sufficient cyber security can lead to malicious aliens entering offices' operating systems. This has the potential to make office networks and infrastructures suddenly vulnerable to cyber-attacks. Canon, the technology company, lists the most serious problems with printer devices used over IOT networks as follows:

- Employees can get someone else's documents from the printer,
- If the printer settings are not checked for security,
- Unauthorized change of documents to be transmitted over the network,
- Monitoring network traffic of cyber hackers leaking into networks via IOT devices,
- Ability to digitally copy documents on un-passworded printers.

2.1 Problems with Intelligent Home Systems

Smart home systems, from heating to lighting in many ways more comfortable and makes the home life easier while increasing energy efficiency also reduces the cost. Other solutions in this area smart alarms and locks increase our security. Smart home assistants such as Google Home and Amazon Echo, though not yet widespread in our country, ensure that all devices in the house communicate and communicate with each other. According to Gartner, in 2020, 25 billion objects in the world will be in contact with each other, and smart home devices will be most of these devices. When you say that, you can think that an extremely comfortable future is waiting for us. But let's look at the empty side of the glass. How safe are these smart home systems that make our lives easier? In this week's article, I've put together the security risks of smart home systems and the simple measures that can be taken.

According to a study conducted in the US in 2016, 47 percent of people do not prefer to use smart devices in their homes yet because they are not sure of their safety. If we go from popular examples again; Amazon Echo and Google Home's voice recording features keep users nervous. In an incident in 2017, the police requested Amazon's Echo records in the house but were confronted by Amazon's objection. Subsequently, the defendant had submitted his own request to be used in his defense. According to another study in 2016, your camera and microphone can be hacked through security vulnerability on Android-based smart TVs. With a malicious application installed on the TV, hackers accessing the device can access other connected devices at home via TV.

Another scary detail on smart home systems is about the WiFi network. Because a WiFi network with security weakness means easy access to the entire system in your home. The best part of smart home technologies is to integrate complex processes and make them manageable from one place. However, the security levels of 3rd party integrations are not yet at the desired level, and this situation makes the smart home systems vulnerable to attacks. Security processes, on the other hand, have become complicated by cyber-hackers' efforts to take home network routers to attack criminals to attack smart home devices. The report, which was shared by Trend Micro in 2017, carried out more than 1.8 million cyber-attacks in the first 6 months of 2017 through home network routers from all over the world. In 8 percent of these attacks, hackers access a home device, run malware remotely, and use confidential information like a password. Other types of attacks; the transmission of content transmitted through the affected devices to the attackers. If we collect the safe risks of smart home systems, we see that the following 3 headings come to the fore: Remaining long time to vulnerable networks, changing passwords and changing the number of home devices, as well as occasional software updates / software updates.

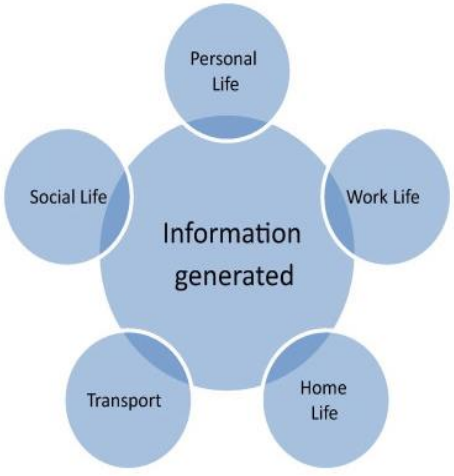
As the dangers and attacks in the cyber world increase, security companies also increase and enrich their proactive approach and solutions. Malicious software is also evolving as hackers implement the encryption method to start using cloud services as a weapon. According to the 2018 Annual Cyber Security Report, which was prepared by Cisco this year, more and more investments will be given to vehicles using artificial intelligence and machine learning to reduce the lifespan of cyber attackers. Cisco researchers, over a period of 12 months, they observed a more than 3-fold increase in the use of encrypted network communications for the malware samples examined.

2.2 Problems with Smart City Applications

All the elements of the smart cities of the future, such as public vehicles, public transport vehicles, traffic lights, street lamps, etc., exchange data with each other online. The city environment created by these intelligent systems can be quite attractive for data thieves. The city of Glasgow has invested € 24 million in smart street lamps and traffic monitoring sensors to facilitate the lives of pedestrians and cyclists. Similarly, the city of Bristol has created a city operating system to collect and interpret data on environmental pollution that threatens community health. It uses. While such cities often use these systems on their main streets, they aim to create a smart city and facilitate the lives of people of the city by spreading them all over the city. However, it is imperative to consider the chaotic conditions that may be caused by a data thief infiltrating the traffic monitoring sensors or the city operating system. Leading security researchers state that open, sensitive data exchanges, such as smart cities, may be more vulnerable to hackers than to computers and smartphones.

The security research company IO Active Labs warned those who governed smart cities by stating that many cities do not plan against cyber-attacks, even though cities have plans against natural disasters such as floods and earthquakes. Intelligent strategies should be developed against cyber-attacks since a human-centered disaster can lead to great devastations.

IO Active Labs, found that 200,000 traffic control sensors from Washington to Melbourne could easily infiltrate pirates. Pirates could exploit these vulnerabilities to manipulate traffic signals or change electronic road signs, such as speed limits, to fatal accidents. Data thieves who exploit vulnerabilities in intelligent systems, such as security systems that can be easily captured, face detection camera systems, can cause large-scale crimes to be committed. Looking at these examples, we can say that a system that is more vulnerable to pirates than a special system would be more attractive. But since all systems are connected in intelligent cities, infiltration of any of the systems with the domino effect can cause a great mess. Therefore, security strategy should be handled and at the same time, all security vulnerabilities for each system should be minimized or even eliminated.



3 Literature Review

As seen in figure 1, a lot of data is being generated. The collections of that data store such as on the device or on a cloud aggregator. This situation causes some risks such as attacks to the stored data. For preventing this issue, several best practices papers published for IOT security best practices recently. The Broadband Internet Technical Advisory Group (BITAG) generated the report about IoT devices based on consumer [1]. The US Department of Homeland Security (DHS) published a document, ignoring things such as personal privacy [2]. The Federal Trade Commission (FTC) released suggestions that stress confidentiality concerns such as notice, data minimization, choice and data safety [3].

Another academic study presents a set of well-investigated Internet of Things (IoT) security guidelines [4].We considered suggestions from all these sources when preparing our article. According to the above studies, to ensure security at IOT devices, devices must be secured, network must be secured, and the overall IOT system must be secured. These headings will be detailed in the security part together with their subheadings.

The following project launched in 2016 in Github. This project is about authentication/authorization feature for Android based Over the Air Firmware update. By using some cryptographic techniques, it developed an algorithm that requires client (android) authentication and authorization before it can go ahead with the OAD update [5].

Another study about IoT security is The Secure IoT Home Gateway [6] in Github. This project improved an innovative solution for safe home gateway.

Some people do a graphical security analysis tool for IoT networks [7] in Github. The name of the project is apparatus software tool. The screenshots of the project is in the Figure 2. We can see all threats and vulnerabilities detailed in this figure.

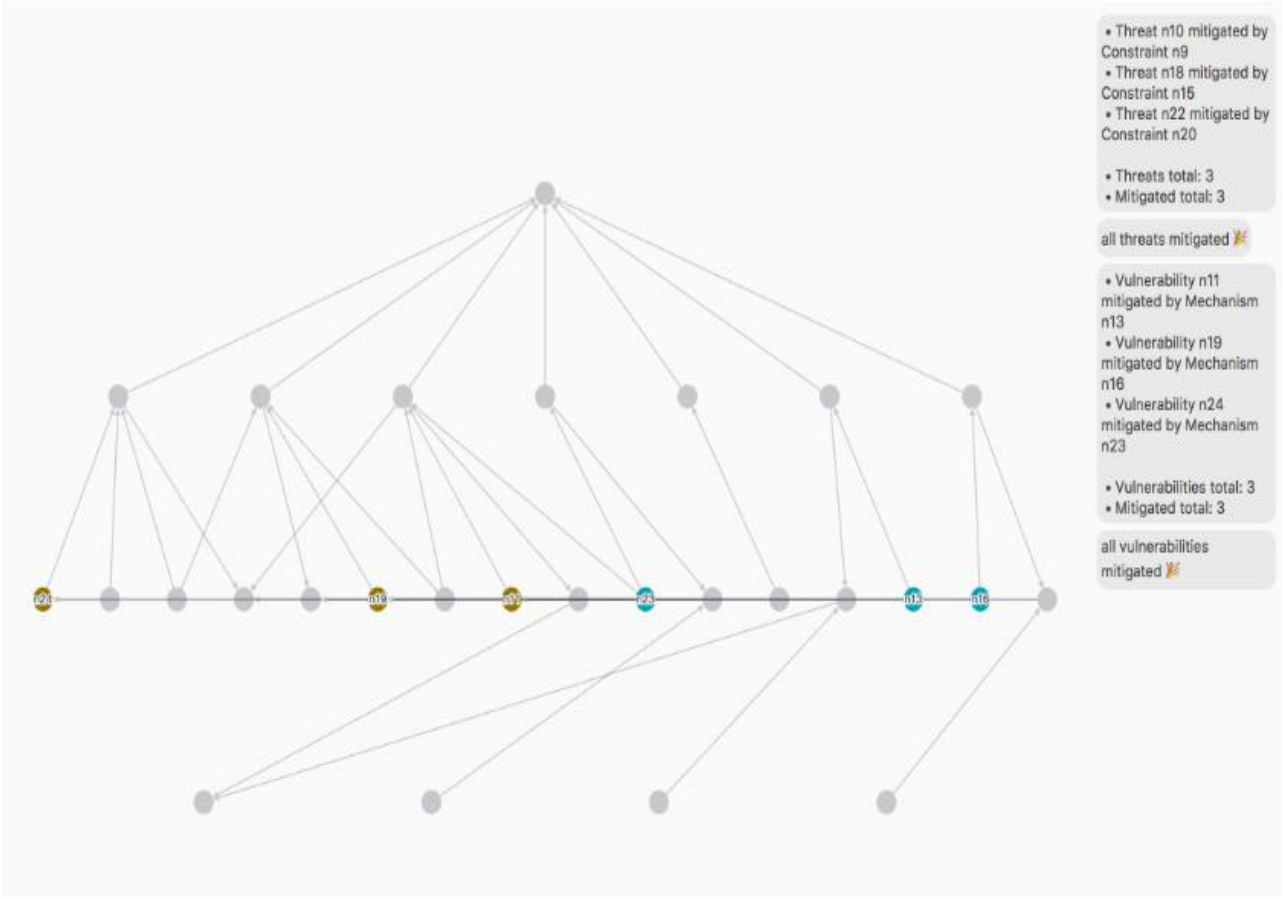


Figure 2. A graphical security analysis

4 IoT Devices Architecture

IoT devices mainly consist of three layers:

- Application Layer
- Network Layer
- Perceptron Layer

Perceptron Layer Attacks:

In perception layer, IOT devices have a strong relationship with sensors, Radio-Frequency Identification (RFID), wireless sensor networks (WSN).

5 IoT Attacks

IoT devices architecture is potentially open to a huge number of attacks. Attacks may be performed at different levels [8]:

• At network level, the hacker has only access to the device through the network or through the applications offered by the IoT solution provider (eavesdropping).

• At device level, the hacker has also access directly to the device, and can perform additional attacks, i.e. invasive or semi-invasive attacks.

• At chip level, the hacker can physically perform attacks on chips located in the device (e.g. reverse engineering).

5.1 Distributed Denial of Service Attacks on IoT Devices

Distributed Denial of Service (DDoS) attacks are defined as a system consisting of many distributed structures is attacking the target. Commonly DDoS attacks are evaluated by considering three layer which are Perception, Network and Application Layer [9] [10]. In table 1 indicates what kind of attacks happens in these layers.

At perception layer RFID is main technology for reading data from sensor without human interaction and touch.

a) Jamming: In this electromagnetic jamming is done to prevent tags from communicating with reader.

b) Kill Command Attack: This kind of attack deactivates communication by using command tag easily.

Table 1. Attacks for different layers

Layer Name	Attacks Name
Perception Layer	Node Capture Fake Node Malicious Data DoS Attack Timing Attack Routing Threads Replay Attack Side Channel Attack
Network Layer	Man in the Middle Attacks DoS Attacks Exploit Attacks Sybil Attacks
Application Layer	Data Access Permission Authentication Software Vulnerabilities Data Aggregation Distortion Data Protection

A new command tag can be protected by password, but anyone can apply a brute force attack and crack it because of limited memory and processing.

The most popular attack on network layer is DoS attacks. On the other hand, on application layer, software vulnerabilities are open to attacks.

5.2 Botnet Attack on IoT Devices

Normally, DDOS attacks with viruses turned into zombies, laptop and desktop computer is via a botnet consisting of. However, this time the hackers have seized the Internet devices of objects: Biggest attacks are on smart phones, smart watches, fitness bracelets, boiler thermostats; smart was made with the Internet of objects, such as lamps

As shown in Figure 3, Botnet attacks are that many computers are managed from a single point in the direction of evil intent.

Malicious hackers set up a community of thousands of zombies and perform botnet attacks via a kind of virus-infected access programs. A Botnet-possessed attacker can easily manage all the computers on his network from any part of the world.

The Botnet attack, which is seen as a dense entry of users, is no different to the normal visitor in the server's eyes. However, when too many user's login and logout to a web site continuously, the server will have to respond to too many requests, and after a while the web site may close because the service band is full [11].

Botnet attacks forms the basis of DDoS attacks. More than one request is simultaneously sent to the target system via the botnet tool to perform DDoS attacks.

5.3 Statistics for Botnet-Aided DDoS Attacks on IOT Implementation

If we need to talk about the quarter results of 2017:

- In the fourth quarter of 2017, DDoS attacks were carried out on target systems in 84 countries.
- The rate of attacks targeting China is over half of all attacks (51.84%).
- The most attacks were occurred against South Korea, China and USA. However, in terms of the number of botnet C & C servers, Russia has come to the fore.
- The longest DDoS attack of Q4 lasted 146 hours in 2017. If we look at previous periods, the longest attack of 2017 (277 hours) was recorded in Q2.
- SYS DDoS is the most popular attack method; the less common method is ICMP DDoS.

Now, we can see the graphs related to the results:

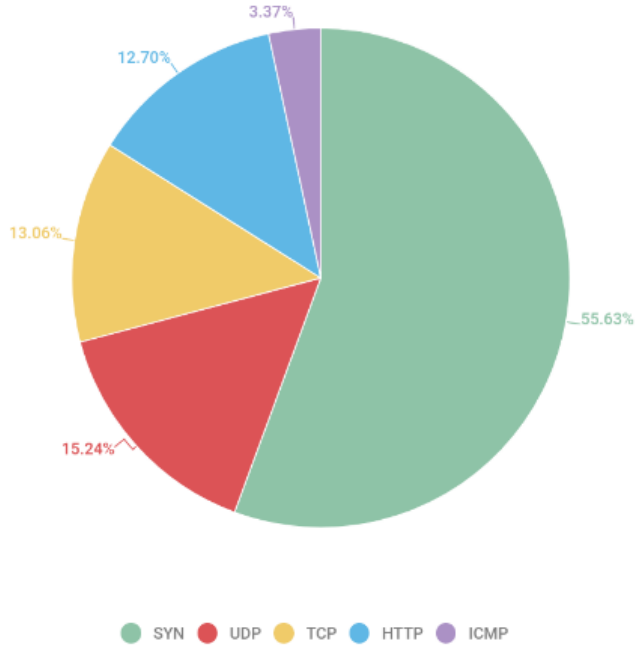


Figure 3. Dispersion of DDoS-attack according to communication protocols - [12]

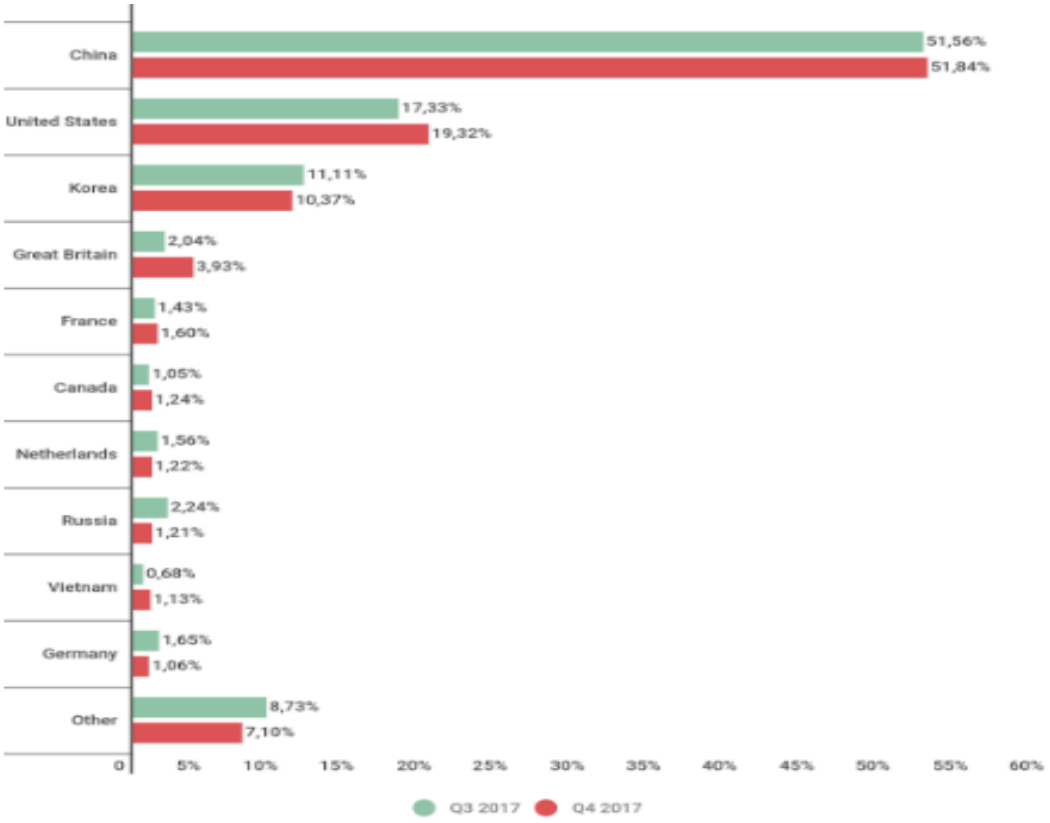


Figure 4. Dispersion of DDoS-attack according to country - [12]

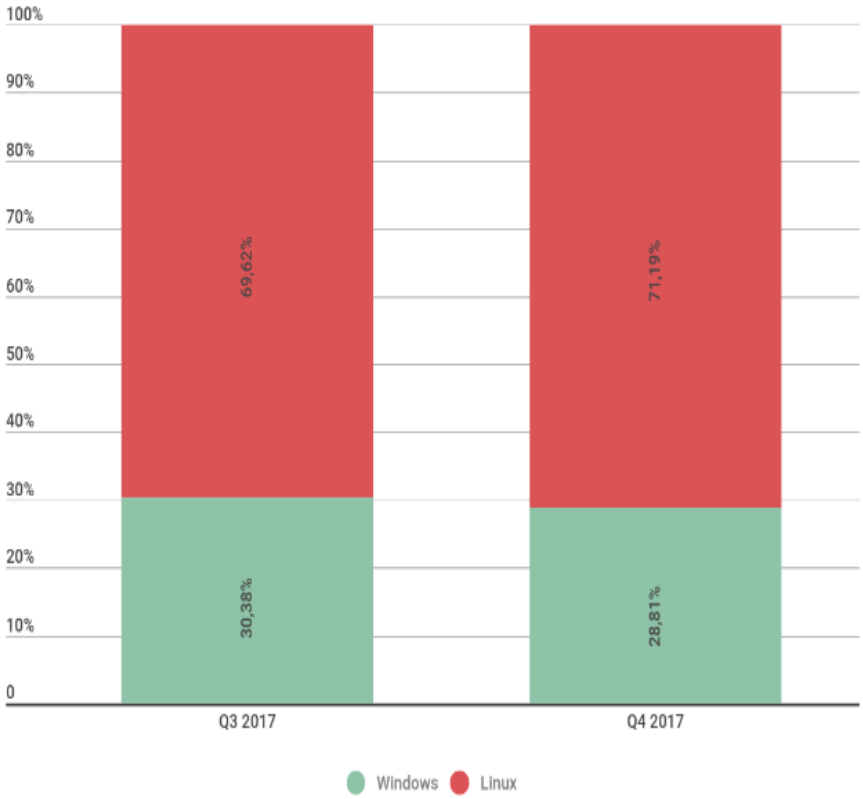


Figure 5. Windows vs Linux-essential botnet attacks – [12]

6 Security of the IoT Devices

We examined the attacks of the IoT devices. In this part, we will examine the security of these devices. This section is separated into three subtitles: security of IoT devices, security of IoT networks and security the full IoT system and is examined each of them detailed.

6.1 Durable hardware

Some these computers may run unsupervised. The IoT system contains a lot of devices. The supervision of these hundreds of computers is very difficult. For this reason, IoT devices takes a lot of attacks as we stated before. For preventing this situation, it is kept these computers isolated thus only a few specific people must be access the system.

6.2 Updating/patching

The computers must be updated in the IOT. New computers are being developed as new cyber attacks. However, no manufacturer 20 years life expectancy is an RFID tag cannot protect future cyber attacks. No firmware will be released after 10 years cannot be prepared to block the malware. That's why we can't protect the internet of objects of the software update.

6.3 Testing

It is the most important that IoT devices pass the testing for the security. But the static testing is not suitable for finding vulnerabilities, because it doesn't find vulnerabilities in processors or memory. For this reason, dynamic testing is necessary for finding these vulnerabilities of these components in IoT.

6.4 Data from removed devices

When the devices are growing old and the user decides to remove of them from the system, these devices must be removing without exposing the data. That is, the data or information in the removed system must be protected.

7 Securing Networks

7.1 Identity

Easy predictable credentials must not use in the IoT system. The computers must not use default username/password information, because once predicted many computer hacks.

7.2 Cryptographic and safe protocols

Even though a computer identity are safe, that is despite user selects strong password and username, contact between devices might be listened. In the IoT there are many protocols, including LoRaWAN, NFC, Sigfox, Bluetooth, Wi-Fi, 6LoWPAN, Neul, Z-Wave, Zigbee etc. According to these protocols, a computer may have necessary to use powerful.

7.3 Separation of the network

For the security of the IoT system, divide the network into segments using IP address ranges etc. These sub networks are used in firewall security to specify one or more source and destination interfaces on the platform.

7.4 Security the full IoT system

The main concept of IoT is to connect objects via Internet; I mean that the devices communicate with each other through the internet. IoT devices ensure services that are explorable by other IoT devices. For preventing the attacks in the internet, only authorized clients should discover the device.

8 Conclusion

Everything in smart homes is connected to the central access point router. Whether your home is fully connected or managed by a single smart device, the first place you need to start improving security is the router. For this, you first need to make your choice of router correctly. The second simple but important setting is to set a new password by changing your router password.

Security must be one of the main criteria in choosing the right device. Some smart device providers can encrypt through the cloud to reduce risks. To avoid the vulnerability, I recommend you choose smart devices that use business applications that work with business partners. If you already have smart home devices, you should learn the features well. For example, if you have features that you do not want / you do not want to change the settings menu, you can personalize the device.

According to the 2015 “Norton Cyber Security Inside Report”, 33 percent of smartphone users do not have a device password. Since smart devices can be controlled via smartphones, your smartphone can be the key entry point to access other devices in your home and the entire system. If your unsecured phone gets in the hands of malicious people, they can interfere with your smart home system as they wish. To do this, first put a password on your smartphone. Another important and necessary step is to install security software on your computer or mobile devices. Because regardless of the security level, all devices can be vulnerable to external attacks.

Managers should take responsibilities to understand the systems they receive while creating intelligent cities and establish transparent relationships with the companies they support from the establishment stage to the maintenance. In addition, every smart city should have trained cyber security emergency response teams against possible cyber-attacks and bad consequences. Not being able to know how to react to the attacks can cause great turmoil, stopping in the usual city life flow. Therefore, serious cyber security strategies should be created. But threats can be re-energized against changing strategies such as bacteria gaining antibiotic resistance. In other words, it is usual to face a new security threat against each improved security strategy. Therefore, security measures should be constantly updated and monitored. In other words, those who want to be protected against attacks should always be a few steps ahead of the pirates.

DDoS attacks can be used easily to IOT infrastructure collapses. For an attack to the diameter, and worst-case scenario; the cities’ or companies’ IT team, for DDoS attacks must develop an effective strategy to prevention. Thanks to the devices used in the form of solutions overprovisioned normal DDoS attacks that exceed your bandwidth, you can manage. For example, a 20 Gbps regular user traffic 1-Gbps bandwidth DDoS attack that uses a device that you can use to have your plan and potential bandwidth is received here by your service provider. If your service provider has to offer the real attack is more bandwidth to work with cloud-based DDoS a considerably increased "scrubber" you may need a hybrid cloud containing.

Segmentation is important for complex smart city IOT networks. For example, the user Smart transport network services, web pages, like other smart energy networks must be a logical way. This helps in isolating segmentation attack and malicious software from a network to another IOT network when switching to the threats the region advanced to be identified. Still, in this way, smart city may be divided into network security zones, and that internal traffic and restricted data and monitoring of devices and resources helps to prevent unauthorized access, use or disclosure.

This type of segmentation is smart city-wide board of IOT equipment only when necessary to communicate with devices and systems and only in designated protocols makes it possible to this communication. In this way, you can also let your internal network is part of a DDoS attack of or the becoming.

To sum up, the attacks of the IoT devices are many. In this article, we examined the Botnet attacks and DDoS attacks and the security of the IoT system in general. For protecting the system for these attacks, emphasized measures must be taken in the security section.

9 References

[1] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations," A Uniform Agreement Report, November 2016. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[2] HC, "strategic principles for securing the internet of things," U.S. Department of Homeland Security, November 15,2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[3] FTC, " Internet of Things: Privacy and Security in a Connected World," *Federal Trade Commission*, 2015. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[4] "Internet of Things (IOT) security best practices," *IEEE Internet Technology Policy Community White Paper*, February 2017.

[5] WIND, "Security for Internet of Things," https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[6] "Secure Home Gateway & Registry Idea," https://github.com/CIRALabs/Secure-IoT-Home-Gateway

[7] "ASTo - Apparatus Software Tool," https://or3stis.github.io/apparatus/

[8] Vault, "IOT Security Solutions," [Online]. Available: https://www.insidesecure.com/content/download/1064/13249/file/IoT%20SecuritySolutions%20White%20Paper.pdf. [Accessed April 2018].

[9] N. Mukrimah, A. Amiza, Y. Naimah and B. L. Ong , "Internet Of Things(IoT) : Taxonomy of Security Attacks," in *International Conference on Electronic Design(ICED)*, Phuket, 2016.

[10] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," in *Ninth International Conference on Computational Intelligence and Security*, Nanning Guangxi, 2013.

[11] Techopedia, "Botnet Attack," Techopedia, [Online]. Available: https://www.techopedia.com/definition/29948/botnet-attack. [Accessed March 2018].

[12] Securelist, "DDoS attacks in Q4 2017," KasperskyLab, [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2017/83729/. [Accessed March 2018].

Authors' addresses

Ahmet Efe 1, PhD, CISA, CRISC, PMP
İnternal Auditor at Ankara Development Agency, Part Time Lecturer at Yıldırım Beyazıt Universiy Ankara/Turkey E-mail: icsiacag@gmail.com

Esra Aksöz 2, MSc Candidate
Yıldırım Beyazıt University, Department of Computer Science, Ankara/Turkey E-mail: esra.aksoz06@gmail.com

Neslihan Hanecioğlu 3, MSc Candidate
Yıldırım Beyazıt University, Department of Computer Science, Ankara/Turkey E-mail: neslihanecioglu@gmail.com

Şeyma Nur Yalman 4, MSc Candidate
Yıldırım Beyazıt University, Department of Computer Science, Ankara/Turkey E-mail: seymanur.ylmn@gmail.com