The Influence of Privacy and Security on the Future of IoT

Mihaela Mădălina ANGHEL, Petru IANC, Marian ILEANA, Laura Iulia MODI
Bucharest University of Economic Studies, Romania
anghelmadalina13@stud.ase.ro, iancpetru08@stud.ase.ro, ileanamarian18@stud.ase.ro, modilaura18@stud.ase.ro

Internet of things (IoT) is a hot topic for study in the last decades. IoT is the internet working of physical devices, vehicles and other objects which consists of an embedded system with sensors, actuators and network connectivity that enable to collect and exchange data. The IoT permits articles to be detected as well as controlled remotely across existing system foundation, making open doors for more coordination of the physical world into PC based frameworks, and result in improved accuracy, efficiency and economic benefit. The IoT is a rapidly increasing and promising technology which becomes more and more present in our everyday lives. Furthermore, the technology is an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes and smart cities. Considering the high-rate improvement of IoT advancements, and the critical addition in the quantity of the associated gadgets, complete diagram of the IoT framework points, design, challenges, applications, conventions, and market outline were examined. In order to give an example of IoT security.

Keywords: *IoT security, IoT Privacy, IOT attacks, IoT future, Internet of Things, blockchain, thingbot.*
DOI: 10.24818/issn14531305/24.2.2020.04

Introduction

The Internet of Things (IoT) refers to the billions of devices around the world that are connected to the Internet, collecting and exchanging data. From toothbrushes to machines, commercial and industrial devices are equipped with chips through which they collect and communicate various information.

From a commercial point of view, many of these objects aim to improve what is known as Quality of Life (QoL), easing people's daily responsibilities. However, they include various less useful devices such as: Egg Minder (a tray that tells you how many eggs you have and how fresh they are) or Shuttereaze (a device that pulls curtains or blinds automatically). [1]

On the other hand, at the industrial level, the interconnection of machinery and apparatus is revolutionizing the market. According to a Gartner report, more than 50% of new businesses will incorporate elements of the Internet of Things.

The combination of device connectivity with systems automation allows the collection of information, its analysis and, implicitly, making a decision based on it. IoT can thus help a person accomplish a task. Moreover, IoT offers devices the opportunity to communicate not only in a private network, but also between different types of networking, thus creating an interconnected world.

How Big is the Internet of Things?

A study also conducted by the Garnter Institute shows that in 2017, 8.4 billion devices belonging to the Internet of Things were used. This represents an increase of 31% compared to 2016, the study also showing that by 2020, their number will reach 20.4 billion. [12]

Of the 8.4 billion, more than half are products such as smart TVs and smart audio systems. According to the same study, the most used devices at the industrial level are smart electric scales and security cameras.

Table 1. Total IoT devices per million units (2017)

Category	**2016**	**2017**	**2018**	**2020**
Consumers	3,963	5,244 (↑ 32,32%)	7,036 (↑ 34,17%)	12,863 (↑ 82,82%)
Businesses: multiple industries	1,102	1,501 (↑ 36,21%)	2,132 (↑ 42,04%)	4,381 (↑ 105,49%)
Businesses: specific verticals	1,316	1,635 (↑ 24,24%)	2,027 (↑ 23,98%)	3,171 (↑ 56,44%)
Total	6,381	8,380 (↑ 31,33%)	11,196 (↑ 33,6%)	20,415 (↑ 82,34%)

What are the investments in IoT?

According to International Data Corporation, spending in this segment will reach $ 745 billion in 2019 internationally, due to developments in production, retail, transportation and utilities. This means an increase of 15.4% compared to 2018, when $ 646 billion was invested.

The adoption of new technologies is visible throughout the industry, in public institutions and in the daily lives of consumers. Device data helps companies operate more efficiently, have a more detailed view of business processes, and make real-time decisions. On the other hand, consumer investments are explained by the increased level of information about their properties (cars, homes), close people, but also about personal health.

What are the benefits of IoT for companies?

Even if the benefits for the business differ depending on the implementation methods, a common denominator can be observed: companies have access to more data on their products and internal systems, thus having a greater ability to make changes.

For example, in the manufacturing industry, various traders introduce sensors into the components of products that transmit data about their performance. In this way, companies can identify when a component is prone to failure, replacing it before it poses a real danger. Moreover, businesses can use the data to streamline their systems and supply chains, with reliable information about how they work.

Considered at the level of an entire supply chain and within a particular industry, the impact can be huge, observable in the exact delivery of materials and in the efficient management of production throughout it. In addition, the Internet of Things can create new sources of revenue for companies. Thus, they can add a predictive maintenance service to the package of a product.

Regarding the type of devices, industry-specific ones (such as sensors in a thermal power plant) are currently the most popular. However, by 2020, inter-industrial products will reach 4.4 billion, and niche products will only reach 3.2 billion. The ranking of IoT investments is driven by production ($ 197 billion), transportation ($ 71 billion) and utilities ($ 61 billion).

What are the benefits of IoT for consumers?

New technologies come with the central promise of making our environment (homes, cars, etc.) smarter, easier to measure and manage. Systems such as Alexa, Google Home, ivee and Mycroft facilitate activities such as obtaining information, listening to music and planning events. Security systems contribute to our security, allowing real-time monitoring of the property.

On the other hand, different sensors can provide accurate information on the degree of environmental pollution, and autonomous cars bring major changes in everyday life. Various devices facilitate interpersonal communication and increase accessibility to various services.

It is important to note at this point that concerns about the security of these systems are currently an important topic of debate. Any object connected to the internet is prone to attacks, and IoT products are no exception to this rule. Moreover, the issues of loss of privacy and ongoing monitoring also enter into discussions about the risk of expanding the Internet of Things.

What is the future of IoT?

We are still at the beginning of what will become an interconnected world. Gradually, both organizations and consumers accept and embrace the changes brought about by the IoT. Consequently, it will be incorporated into every aspect of our daily lives.

Both personally and professionally, we will be connected to this network of devices, which will thus become not only a part of our future, but our future itself.

2 Privacy and Security in IoT

A secure network is extremely important in preventing malicious attacks, as it provides an access gateway to the server where the application is stored. The safest way to prevent attacks is to secure the network to avoid invalid requests from outside. Among the most common network common threats we find sniffing, spoofing, information gathering and denial of service (DoS).

Intercepting and monitoring network traffic is called **network sniffin**. Private information can be transmitted in forms as plain text, visible passwords or with a weak encryption, and then will be taken easily by network attackers. To prevent network sniffing, it is necessary to provide a complex system for encrypting passwords, prevent sniffing devices from accessing the network, monitor devices from network and all the programs installed on them. It is important to ensure a permanent monitoring and security of the network traffic.

Creating false identities of the packages is called **spoofing**. They can be used to hide the identity of services attacks or to take over an identity that has access to the private area of the network. To prevent spoofing attacks, it is necessary to include a filter on all entries (filter all the requests based on their IP from a certain network) and egress filtering (cancelation of the sending of requests to an external server that is not on a strict whitelist). If one knows the list of IP addresses that come from a certain network that can be trusted, ingress filtering can be used. This type of filtering is most often used to remove packets coming from foreign networks disguised as IP addresses that come from a trusted network. On the other hand, egress filtering requires more configuration work, so it is useful for large networks with a high level of security.

The attempt to obtain information about the system that may reveal weaknesses and other vulnerabilities is an **information gathering** threat. Attackers may search through your ports looking for open ones. They can collect information about the operating system running on the network and about the software products used, along with their versions. If it is used a version of the operating system or software with vulnerabilities, they will launch an attack on the network using that information. To prevent such attacks, it is recommended to use a firewall to block services that are not indicated to be publicly exposed and to use generic service banners that will make public only those information considered safe about services.

However, the most common forms of network attacks are **DoS (Denial of Service)** attacks. In the US, for example, DoS has been the most frequent attack since 2010 [11]. The intent of this type of attack is to prevent users from accessing the server where the web application is hosted. Most DoS attacks combine sending packet floods to the server with overloading attacks, but there are others that are based on application and operating system vulnerabilities (for example, some older operating systems do not cope with a teardrop attack). To prevent DoS attacks, it is recommended to properly configure the firewall, routers, switches and always upgrade to the latest version with all security measures implemented for services, applications and operating systems.

Best practices for router security implies blocking all unused ports, disabling all unused services and interfaces, updating the router's operating system with all security patches up to date and recording suspicious activities in a log file.

To ensure the security of the switches it is necessary to encrypt the traffic and to deactivate all unused services and interfaces.

For firewall security it is recommended to record all activities, place firewalls between unreliable sources and enable packet filtering.

Securing the IoT

The IoT infrastructure must be immune to an attack like the ones listed above. To prevent this, access control systems will be implemented to limit access only to verified users by integrating strict authentication measures and security safeguards will be included.

We can take the example of medical control devices. The manufacturers prevent the deterioration of these devices by imposing mandatory digital signature for all files and by removing unofficial accounts. The initial credentials for accessing IoT devices must also be renewed.

It is necessary to use a complex security system (for example, intrusion detection and prevention systems, antivirus software) to protect devices and prevent threats. An example of Bitdefender antivirus that can protect daily devices from malicious software. [2] However, the same level of security is not required for every IoT device. The level of security chosen must be applicable with the threats that may arise from those information transferred, collected or stored.

Comparison of Security of IT devices and IoT devices

The connection rate of physical devices to the internet is growing rapidly. Their number is expected to increase to 20 billion by 2022, according to the Gartner report. The use of IoT applications is constantly increasing in all parts of the world, especially in North America, China and Western Europe. The number of machine to machine connections will increase to 27 billion by 2024. [6] This growth makes the IoT one of the main markets that will contribute to the expansion of the digital economy. IoT market revenues can grow to $ 4 billion by 2025. Machine-to-machine connections apply to a wide range of applications, such as smart retail, smart cities, smart environment. [7]

In the future, devices are expected to communicate with another devices directly over the Internet. The concept of SIoT (Social Internet of Things) is also present, because it allows users to connect devices to different social networks and share them on the Internet.

The wide range of IoT applications raises the issue of privacy and security. IoT applications cannot meet high demand and therefore can lose their potential without a feasible and reliable IoT ecosystem. In addition to common Internet security threats, there are also present its own security challenges such as authentication and privacy issues, information storage, management issues and so on.

Table 2. Security of IT devices vs IoT devices

IT Security	**IoT Security**
Global IT has its origin in devices with substantial resources	IoT system are compound of devices with limitations regarding their hardware and software
Global IT has resourceful devices	IoT devices must be rigorously supplied with security measures
Complex algorithm are executed for lower capacities and extensive security	Lightweight algorithm are used
High level security produced from similar technology	Similar technology increase the attack surface from producing large amount of heterogeneous data

Table 2 highlights various factors that determine the security of IT devices and IoT devices. We notice that ensuring security in IoT is more difficult than for normal IT devices. Due to these vulnerabilities, IoT applications are more predisposed to cyber attacks. Being less secure and having less power, IoT devices offer attackers an entrance into home and corporate networks, then can have easy access to users confidential information. The IoT domain has tried to expand apart from common things or objects. Successful experiments have been recorded to implant IoT devices into the human body to monitor various organs. [8] These devices can be targeted by attackers to track the individual's location and falsify information. If the devices are compromised, such an attack can be very dangerous.

IoT Security using blockchain

Blockchain is an important technology that can have a huge impact on the IoT applications. It focuses on improving the level of trust and comfort for users. IoT devices provide real-time data from sensors and blockchain is in charge of their security using a decentralized and distributed registry. The principle of blockchain is simple: a distributed ledger. The log files are recorded chronologically and each entry from the registry is closely paired with the previous one by cryptographic hash keys. The ledger maintainer checks the entries and generates a key that allows the latest transaction to become part of the register. This process makes the latest transactions available to all nodes in the network. Because each block has cryptographic hash keys, the process is time consuming and therefore difficult for attackers to interfere with blocks. [9]

Depending on the type of data added and the application, there are two types of blockchain: without and with permissions. In permissionless blockchain, anyone can be part of the network, no permissions are required for the user to be a miner (for example Bitcoin).

But the permissioned blockchains have a defined set of rules for the user to participate in the blockchain network. Data blocks can be added only after the validation from the authorized persons (the miners). The applications that use this type of blockchain are Hyperledger and Ripple. Compared to the one without permissions, this one improves the overall transfer of the transactions.

IoT Security using fog computing

Cloud computing and IoT are two separate technologies that include a large number of applications. The cloud offers a useful solution in managing and storing data that can be accessed from anywhere. IoT generates an unusual amount of data, so the internet infrastructure can be affected. The union of IoT and cloud raises new opportunities and challenges related to managing, storing, processing and securing data. Several industries have tried to solve some problems in IoT by integrating with the cloud. That's how the concept of fog computing was introduced.

Fog computing manages the data generated by IoT devices for better management. It requires an architecture divided into several layers. It contains two frameworks: Fog-Cloud-Device framework and Fog-Device framework. [10]

Layers are arranged based on their storage and computational capacity. Communication between them is done using wired or wireless communication. In the Fog-Device framework the nodes offer various services to the users without the involvement of cloud servers, and in the Fog-Cloud-Device framework the complex decisions are taken on the cloud and the common ones are taken at the fog layer.

Risk versus reward

Everything we use will collect information about everything we do. We may have to sacrifice the very concept of privacy on the altar of unlimited connectivity. Since all aspects of our lives will be connected, the idea that someone, an organization or a government will want to know all our habits and every move we make is not hard to believe.

But there is another danger that may not be visible at first. Having so many smart devices around us means that a hacker could compromise their security and even turn them into extended networks of bots to launch access ban attacks. These devices could also be subject to attacks for damages. Just these days, the city of New Orleans declared a state of emergency due to ransomware attacks that blocked its activity. However, weighed against the benefits, the risks may seem minor, because without interconnectivity, life in big cities has all the chances to become unbearable. In other words, it is not a future we can avoid, even if we want to. [3]

Basic design

The basic design for the network (Fig. 1) can be the flow of data and messages of messages with their care are sent between users and devices. Each object is required to have process-specific steps, including users, devices, and software. Dotted lines require the general structure of authentication; network interactions, applications, people and hardware; and also to identify possible attack positions. The changed packages include network searches, access control processes, data logs, and real-time information. The aim of the project is a visualization of a clear arrangement model, as can be seen in Fig. 1.

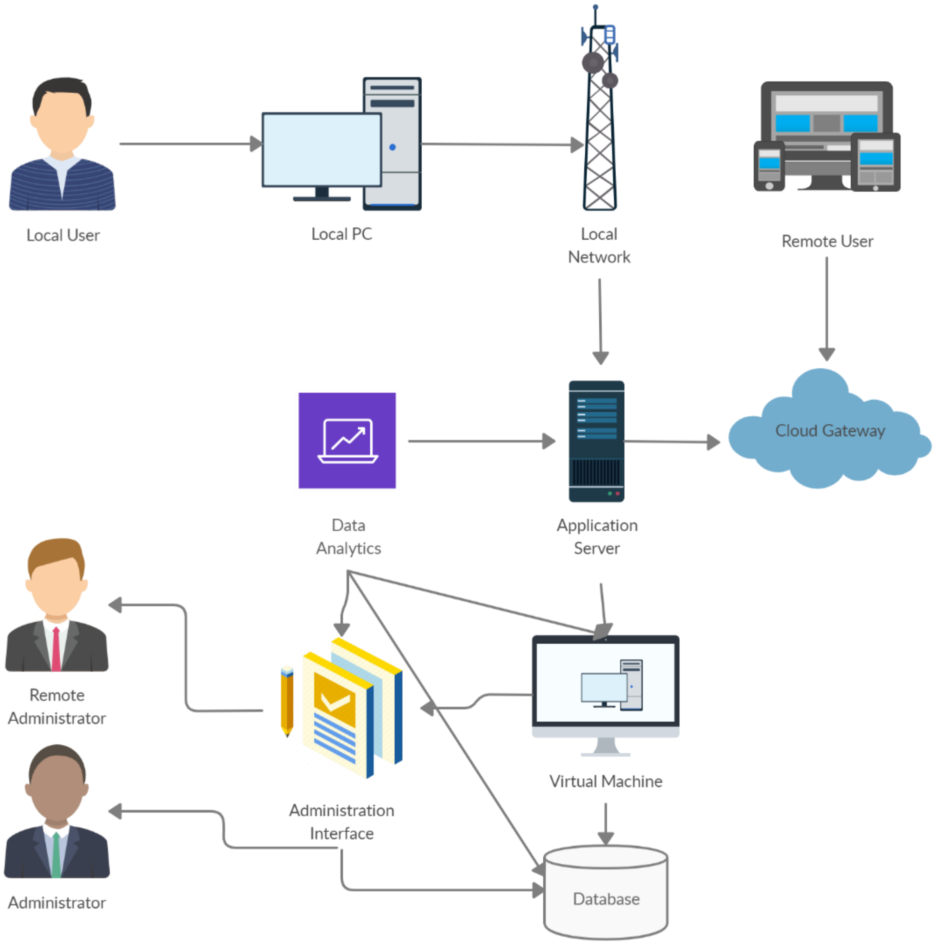


Fig. 1. IoT Network Architecture

Top 10 IoT Security Issues

The primary purpose of the Open Web Application Security Project (OWASP) is to disseminate best practices that lead to improved software security. It is natural to analyze the 10 most important security issues for this popular paradigm.

1. Insecure web interfaces
2. Insufficient authentications / authorizations
3. Insecure network services
4. Lack of encryption on data transport
5. Privacy issues
6. Unsafe cloud interface
7. Insecure mobile interface

8. Insufficient security configurability
9. Unsafe software/firmware
10. Low physical security

1.Insecure web interface:
Almost any device has a web server implemented for maintenance purposes, but in most cases the internal server interfaces are not secure. Weak authentication mechanisms, CSRF, XSS and SQL injections are the most common vulnerabilities affecting web servers.

2.Insufficient authentications / authorizations:
Security experts should carefully check for strong passwords and avoid hard-coded credentials. Another aspect is the verification of common vulnerabilities (e.g. sqli) for authentication/authorization processes.

3.Insecure network services:
SSH, SFTP and other services must be properly implemented. A common mistake in these situations is the hard coding of service credentials.

4. Lack of encryption on data transport:
Credentials and data must be encrypted. The adoption of the PKI should help administrators implement effective information security processes.

5.Privacy issues:
It is important to consider all aspects of the IoT architecture that could expose sensitive unencrypted data.

6.Unsafe cloud interface:
IoT devices can be integrated with cloud services for data sharing. The interface with cloud services must be properly implemented and designed to avoid the presence of critical vulnerabilities.

7.Insecure mobile interface:
Many smart devices provide "Wireless Access Point" functionality, such as smart TVs, and a strong encryption algorithm and security best practices (eg disabling SSID transmission) are required.

8.Insufficient security configurability:
IoT devices must be able to configure the main security features required by security policy compliance.

9.Secure software/firmware:
Make sure that the firmware and software running on the devices can be updated and that the upgrades are done through secure processes that avoid modification/replacement. Avoid software/firmware that has hard-coded credentials and a good practice is to validate the software by digitally signing the source code.

10.Low physical security:
Check the physical security of smart devices by protecting access to all exposed ports. Manufacturers usually provide external access for maintenance purposes. An attacker can exploit one of these access points to inject malicious code, filter data, or sabotage the smart object. It is suggested to encrypt the data stored in the device memory and physically protect the USB ports and any other port by disabling unnecessary access.

Attack scenarios
Security firms have seen an escalation of cyber attacks on IoT devices on a global scale. The most common scenario is the use of botnets made up of thousands of IoT devices, also known as thingbots, which are used to send spam or coordinate DDoS attacks. Summarizing a thingbot can be used to:

- to send spam.
- coordinate an attack on critical infrastructure.
- to provide malware.
- to function as an entry point into a company's network.

Major security firms confirm an increase in the number of attacks on smart objects, including routers, Smart TVs, devices NAS (network-attached storage), game consoles and various types of set-top boxes.

One of the first large-scale attacks was reported by researchers at Symantec in November 2013, when a worm named Linux. Darlloz infected many Intel x86 devices running Linux by exploiting various vulnerabilities in PHP.

The worm managed to compromise internet kits for the home, equipped with x86 chips, to exploit them and spread the infection. The malicious code compromised network equipment globally, as described by Symantec in a detailed report.

"The Linux worm. Darlloz exploits PHP vulnerabilities and spreads itself. The worm uses the vulnerability known as PHP "php-cgi" Information Disclosure Vulnerability (CVE-2012-1823), which is an old vulnerability for which there is a patch from May 2012. The attackers recently created a worm based on the code Proof of Concept (PoC) available from the end of October 2013 ", it is stated in a post on the Symantec blog.

Although the worm was designed to compromise Intel x86 devices equipped with Linux, Symantec experts found that there is also a Darlloz version compiled to run on ARM and MIPS devices. Darlloz managed to spread quietly and partially delete files stored on IoT devices.

The attack technique was simple and effective, the malicious code generated random IP addresses and tried to use commonly used credentials to log in to the target machines. If the malware identifies a vulnerable device, it accesses and downloads the worm from a server. Once the IoT device became infected, the malware began searching for other targets running a web server and PHP.

Darlloz uses HTTP POST requests specifically designed to exploit vulnerable devices. Once the malware identifies a non-patch device and takes control, it downloads the worm from a server and starts searching for other targets by running a web server and PHP.

To prevent the device from recovering, the worm stops the Telnet services running on the smart component, making it impossible to connect remotely to it to return it to normal operation.

A few months later, in January 2014, researchers at Proofpoint discovered another misuse of IoT devices, with more than 100,000 refrigerators, smart TVs and other smart home devices being hacked to send 750,000 e-mails. malicious spam.

"The attack observed and profiled by Proofpoint took place between December 23, 2013 and January 6, 2014, and consisted of sending waves of malicious e-mails, in series of 100,000, 3 times a day, to companies and individuals globally. More than 25% of this volume was sent through items other than conventional laptops, desktops, or mobile devices; e-mails being sent by consumer gadgets such as home routers, connected multimedia centers, televisions and at least one refrigerator. ”

Meanwhile, the attacks continue, recently experts from the Akamai Prolexic Security Engineering & Response Team (PLXsert) reported a new malware kit called Spike, which is used to launch DDoS attacks via desktops and IoT devices.

The Spike Thingbot is capable of launching various types of DDoS attacks, including SYN, UDP, Domain Name System requests, and GET floods against Linux machines, Windows, or ARM hosts with Linux.

The thingbot consisted of home routers, smart dryers, smart thermostats and other devices Smart. Akamai noted that the number of devices that made up the Spike botnet ranged from 12,000 to 15,000, with researchers highlighting the attackers' ability to customize malware for ARM architectures widely used by IoT devices.

"The ability of the Spike toolkit to generate attacks on ARM architectures also suggests that the authors of these tools target devices such as routers and IoT devices to extend their botnets for a post-PC era of botnet propagation," the statement said the Akamai document.

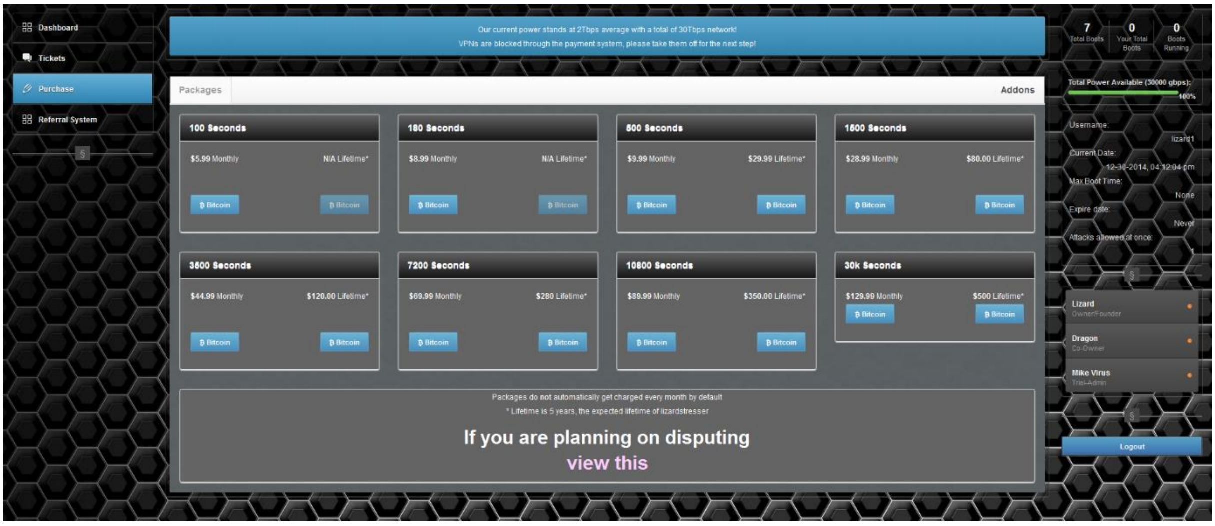
The Spike botnet has been used for several "hit and run" DDoS attacks involving both Windows and Linux machines, IoT and Raspberry Pi devices. Experts have noted that the new influx of Spike malware was based on an update to the Chinese Spike malware language targeting poorly configured Internet-of-Things devices.

Akamai has released an interesting report on the Spike botnet that includes details about the DDoS attacks that took place. Experts noted that one of the attacks included tactile packets at 215 gigabits per second (Gbps) and 150 million packets per second (Mpps). The document confirms that even if most DDoS attacks are launched from low-power devices, and may seem insignificant, IoT devices can be a powerful weapon in the hands of attackers. "Several Akamai customers have been the target of DDoS attacks launched by this botnet. An attack had a peak of 215 gigabits per second and 150 million packets per second", [12] the company document states.

The list of cyber attacks on IoT devices is very long, one of the strongest attacks happening at Christmas, when the popular gaming platforms Sony PSN and Xbox Live were blocked by an attack by a group of hackers known as Lizard Squad.

The group used a DDoS tool called Lizard Stresser in the attack, according to security expert Brian Krebs, which consists of thousands of hacked home Internet routers.

Lizard Squad also recently developed a commercial offer for Lizard Stresser, which offers for sale an attack-as-a-service model and the hacking of IoT devices allows criminals to easily manage such offers.



Our current power stands at 2Tbps average with a total of 30Tbps network!
VPNs are blocked through the payment system, please take them off for the next step!

100 Seconds
$5.99 Monthly N/A Lifetime*
₿ Bitcoin ₿ Bitcoin

180 Seconds
$8.99 Monthly N/A Lifetime*
₿ Bitcoin ₿ Bitcoin

600 Seconds
$9.99 Monthly $29.99 Lifetime*
₿ Bitcoin ₿ Bitcoin

1800 Seconds
$28.99 Monthly $80.00 Lifetime*
₿ Bitcoin ₿ Bitcoin

3600 Seconds
$44.99 Monthly $120.00 Lifetime*
₿ Bitcoin ₿ Bitcoin

7200 Seconds
$69.99 Monthly $280 Lifetime*
₿ Bitcoin ₿ Bitcoin

10800 Seconds
$89.99 Monthly $350.00 Lifetime*
₿ Bitcoin ₿ Bitcoin

30k Seconds
$129.99 Monthly $500 Lifetime*
₿ Bitcoin ₿ Bitcoin

Packages do not automatically get charged every month by default
* Lifetime is 5 years, the expected lifetime of lizardstresser

If you are planning on disputing
view this

7 Total Boots | 0 Your Total Boots | 0 Boots Running

Total Power Available (30000 gbps): 100%

Username: lizard1
Current Date: 12-30-2014, 04:12:04 pm
Max Boot Time: None
Expire date: Never
Attacks allowed at once: 1

Lizard Owner/Founder
Dragon Co-Owner
Mike Virus Trial-Admin

Fig. 2. Dashbord Lizard Stresser

The Lizard Stresser tool is a powerful DDoS tool that takes advantage of the internet width of global hacked home Internet routers. In September 2014, experts at Kaspersky Lab discovered a hacking campaign led by attackers in Brazil targeting domestic routers through a web attack.

Attackers adopt different techniques, including social engineering and malicious websites, to change the DNS settings of home routers. Attacks by changing DNS settings allow attackers to redirect victims to fake websites to steal bank credentials from Brazilian banks' customers. In March 2014, researchers at Team Cymru published a detailed report on a large-scale SOHO farm attack that affected more than 300,000 devices globally.

Unfortunately, criminal groups are increasingly looking at IoT networks in order to compromise them and launch DDoS attacks.

In most situations, IoT devices lack defensive measures and their software is not up to date, circumstances that cause these powerful objects to be exposed to cyber attacks.

A few weeks ago, experts from the security company Imperva Incapsula discovered a DDoS botnet consisting of tens of thousands of malware-infected SOHO routers engaged in a flood attack at the HTTP application level. SOHO routers were infected with a Trojan version of Linux Spike (Trojan. Linux.Spike.A) and MrBlack, which is a Linux agent first reported by researchers at Dr. Web in May 2014.

The attackers facilitated remote access to SOHO routers via HTTP and SSH on their default ports, to compromise them. As explained in the report published by Incapsula, SOHO routers were poorly configured, with attackers using default credentials (eg: admin/admin) to access and inject malicious code. The malware managed to self-propagate by scanning the network to locate and infect other routers. According to the researchers, the hijacked

SOHO routers were devices on ARM architectures from the wireless network equipment manufacturer Ubiquiti Networks.

The company discovered a series of attacks against its customers at the end of December 2014, in a period of 121 days in which they monitored the malicious architecture used by criminals. The IPs of 60 command and control (C&C) servers were identified and malicious traffic was launched from over 40,000 IP addresses belonging to nearly 1,600 ISPs in 109 countries on all continents.

It is interesting to note that over 85% of infected SOHO routers have been located in Thailand and Brazil.

"Over 85% of compromised routers are located in Thailand and Brazil, while most control centers are located in the US (21%) and China (73%). In total, we documented attacks from 109 countries around the world", the report said. [5]

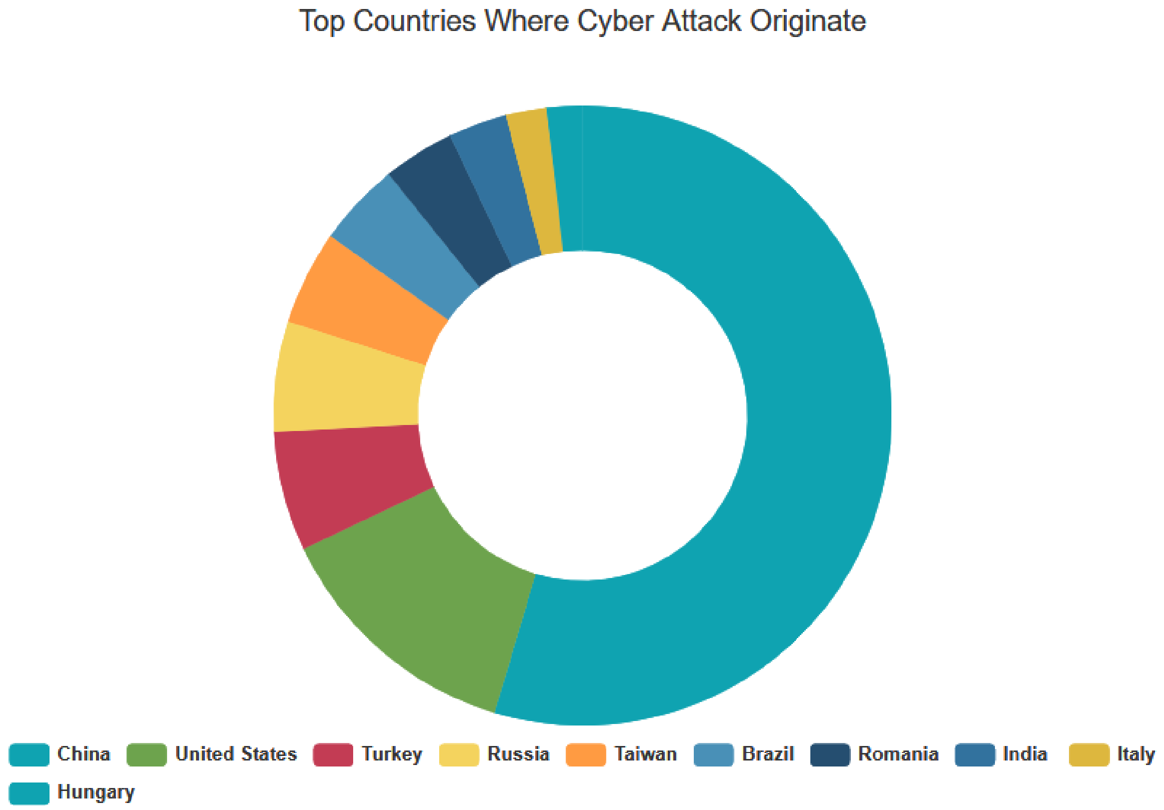


Fig. 3. Top Attacking Countries

According to Incapsula, the compromised SOHO routers have been exploited by several groups, including the popular group Anonymous. The encapsulation speculates that hundreds of thousands or even millions of SOHO routers have been compromised due to poor configuration.

Bash Bug, Heartbleed and the Internet of Things

Bash Bug (CVE-2014-6271) is a critical bug that can be exploited remotely and affects Linux, Unix and Apple Mac OS X machines. Bash Bug has been around for decades and is related to how bash handles variables specially formatted environment, namely the exported shell functions.

In order to run an arbitrary code on an affected system, it is necessary to assign a function to a variable, the code hidden in the function definition will be executed.

The Bash Bug defect impacts billions of devices around the world running Linux/Unix architectures, including IoT devices.

Security companies confirm that the Bash Bug vulnerability could already be used by criminals to damage devices in various industries.

The main problem in addressing IoT devices is that in many scenarios the maintenance of such objects is very difficult and that sometimes manufacturers do not provide security updates to eliminate the problems, leaving them accessible to cyber attacks.

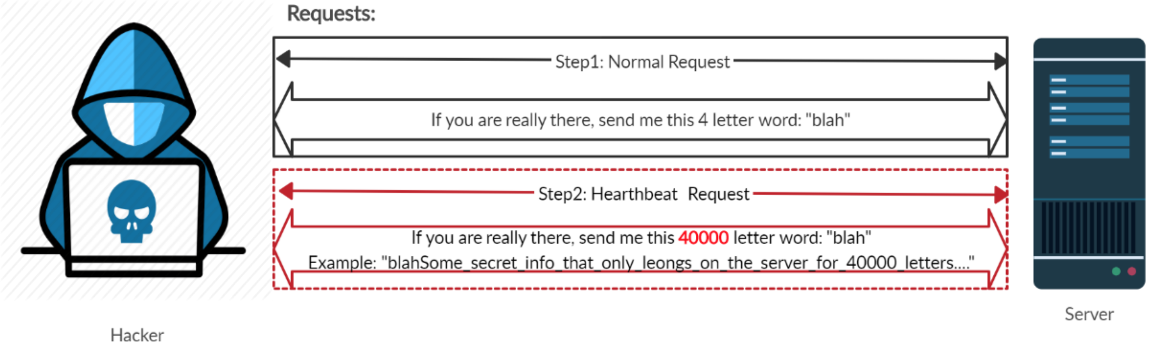

Requests:
Step1: Normal Request
If you are really there, send me this 4 letter word: "blah"
Step2: Hearthbeat Request
If you are really there, send me this 40000 letter word: "blah"
Example: "blahSome_secret_info_that_only_leongs_on_the_server_for_40000_letters...."
Hacker
Server

Fig. 4. Heartbeat attack

Another vulnerability that threatens IoT is the popular Heartbleed, which can affect routers, PBXs (business phone systems) and many other smart objects.

By exploiting the Heartbleed defect, an attacker can remotely read the memory of systems running vulnerable versions of the popular OpenSSL library.

A vulnerable IoT device connected to a server can be compromised if it is affected by a Heartbleed vulnerability by simply sending a malicious Heartbeat message to it. The IoT device will respond by sending additional data from its memory, and may expose credentials and other sensitive data.

The good news, as explained by Symantec researchers, is that although Heartbleed attacks on a server are not complicated to perform, a large-scale offensive on some customers is difficult to run in a real-world scenario. The two main attack vectors for exploiting the Heartbleed defect in IoT devices are determining the smart object to visit a malicious SSL/TLS server or by hijacking the connection through an uncorrelated weakness. In both cases, the attacks are more difficult for criminals to carry out.[4]

5 Conclusion

IoT is a paradigm that will influence our lives in the years to come. for this reason, it is essential that security and privacy issues are properly addressed. Security experts urge manufacturers and vendors to consider the cyber threats and the level of exposure of any IoT device. IoT provides business opportunities to every industry, but can become a nightmare if security components are underestimated.

References

[1] M. Miller, *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing The World*. Indianapolis. pp 80-84.

[2] M Wood, *At the International CES, the Internet of Things Hits Home* New York Times, (2015, January 4) http://www.nytimes.com/2015/01/05/ technology/international-ces-the-internet-of-things-hits-homes.

[3] Cisomag (2019, December 17) retrieved from https://www.cisomag.com/new-orleans-declares-state-of-emergency-after-ransomware-attack/

[4] *Heartbleed bug leads to forking and funding* https://doi.org/10.1016/S1353-4858(14)70045-5

[5] Hwansoo Lee, *Home IoT resistance: Extended privacy and vulnerability perspective* https://doi.org/10.1016/j.tele.2020.101377

[6] Rajesh Kandaswamy, *Blockchain-based transformation*, https://www.gartner.com/en/doc/3869696-blockchain-basedtransformation-a-gartner-trend-insight-report/, online; (2018, June).

[7] P. Fraga-Lamas, *A review on the use of blockchain for the internet of things*, IEEE Access, vol. 6, pp. 32979– 33001, 2018

[8] G. Yang, *Iot-based remote pain monitoring system: From device to cloud platform*, IEEE journal of biomedical and health informatics, vol. 22, no. 6, pp. 1711–1719, 2018.

[9] H. Orman, *Blockchain: The emperors new pki?*, IEEE Internet Computing, vol. 22, no. 2, pp. 23–28, 2018.

[10] S. Shen, *Securing fog computing for internet of things applications: Challenges and solutions*, IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2018.

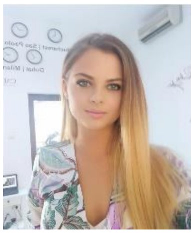
[11] Headlines, *DDoS Attacks Against Government and Entertainment Websites Escalate* (2012, January 19), retrieved from http://www.infosecisland.com/blogview/19543-DDoSAttacks-Against-Government-and-EntertainmentWebsites-Escalate.html

[12] Granter (2017, February 7) Retrieved from https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Mihaela Mădălina ANGHEL has graduated the Faculty of Economic Cybernetics, Statistics and Informatics, Economic Informatics specialization, in 2018. She holds a Master diploma in the research of Economic Informatics from 2020. Her current interests are new technologies and client-side web development.

Petru IANC holds a Bachelor’s degree in Business Administration from the Bucharest University of Economic Studies. He studied statistics for one year at the Duisburg-Essen University in Germany. He is currently studying for a master’s degree in Economical Informatics at the same academy. Petru’s current interests are Java web-development and client-side angular development.

Marian ILEANA has graduated the Faculty of Mathematics and Computer Science, Computer Science specialization, in 2017. He holds a Master diploma in the research of Economic Informatics from 2020 and a Master diploma in the professional of Databases and Web Technologies from 2020. His current interests are in the development of hybrid mobile development and autonomous database.



Laura Iulia MODI has graduated the Faculty of Economic Cybernetics Statistics and Informatics, Statistics and Forecasting specialization. She studied for four months at Puskin University, Moscow. Now she is studying for a master’s degree in Economical Informatics Master at ASE Bucharest and she is currently working for IBM as a SQL developer.