International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Challenges, Risks and Measures to Prevent Threats in Iot Security

N. Sivashanmugam

Tnou

Abstract:
This paper discusses the problems related to ensuring their functionality in the environment of increasing the trends in IOT development and such systems to increase cyber threats. Their widespread use in industries, services and other fields, Incl. Administration increases the risks of unauthorized access to resources of various local and corporate networks as well as desktops, web servers, database etc. The article is an attempt to organize the methods of risk analysis and organize ways to prevent them. Recent developments in IOT hacking practices, such as ransomware, ddos, botnets and others, have also been reported. This issue is focusing on how to compromise and often prevent the entire production units from topping the elements or the entire infrastructure system.

Keywords: hacking, iot, network, threats, security, system, vulnerability

1. INTRODUCTION

Why is IOT becoming the most popular? Their owner and use create new opportunities and both average consumer and business get an advantage. This creates a lot of opportunities for businesses to develop new services and products, create incredible features and give more satisfaction to your customers. Initially focused on individual user requirements, the IOT application in business is currently exceeding our wild dreams. For example, those shipments were added, which automatically update their logistics system, when connected to the recipient's local network. In IOT medicine, the sensors are connected to the patient, show real -time data on basic important functions and allow distance action. In short - the possibilities of use are unlimited, as well as the number of devices that can be connected. But although the ecosystem connected in 2019 is quite wide, it is ready to grow even more in the coming years. We are at the peak of an era when almost everything around us has some forms of internet capabilities, such as home appliances, cars, office equipment, urban infrastructure and healthcare equipment.For many, the Internet of Things (IoT) will mark the next great revolution for humanity. According to Statistics, there will be 31 billion Internet-connected devices by 2025, and Gartner predicts that the average family home will have 500 smart devices by 2022. Meanwhile, IDC claims that IoT costs will reach $ 745 billion in 2019.

Some of the advantages of IoT include the following:

- ability to access information from anywhere at any time on any device;
- improved communication between connected electronic devices;
- transferring data packets over a connected network saving time and money; and Automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

2. How IoT works

An IOT ecosystem consists of web-capable smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and function on data obtained from their environment. The IOT devices share the sensor data collected by connecting to an IOT gateway or other edge devices, where the data is either sent to the cloud or analyzed locally. Sometimes, these devices communicate with other related devices and work on the information obtained from each other. Tools work mostly without human intervention, although people can interact with equipment - for example, to set them, direct them or access the data. Looking inside, there are six IOT network architecture components: The IoT device itself It could be a sensor, an MRI machine in healthcare, an actuator etc.

- Communication -- how a device communicates its data. There are two basic enterprise network architectures that address IoT network communication infrastructure requirements for IT organizations: wide-area communication and cloud application or on-premises communication, according
- The third framework component is security. Security technologies are necessary to protect IoT devices and platforms from breaches. Connected devices that have been in use for many years must communicate safely and securely with newer connected devices.
- The fourth IoT network gateway. Gateways can house the application logic, store data and communicate with the internet for the things that are connected to it, according to Gartner.
- The fifth component is the IoT platform, which is an aggregation point for one or multiple different sites or products.
- The last component is the application, which is kind of the user interface. The application component uses collected data to enable users to monitor and control their cars or smart homes, for example.

3. Security issues

Despite the capacity of IOT, several risks should be considered during the creation of such infrastructure. Because these are the equipment designed to connect to the web, their operating system is made in their firmware. Due to this fact, these embedded operating systems have not been designed as a priority and paramount idea with antivirus security, which is why their vulnerability for cyberlack is present in almost all. The most recent example is an avalanche of malware that targets Android-based devices. As soon as they log in to any network, similar dangers are likely to spread in IOT. With dangers in the age layer (sensors, actuators, devices), classic attacks and application software in the communication section - viruses, phishing, botnets, theft and data destruction - are increasing. Hackers are using connected tools to collect sensitive data, send spams, monitor network and launch cyber attacks worldwide. Bottnet attacks have become common, in which the Centurelink Threat Research Lab estimates that 195,000 such attacks occur each day, and the average costs the average cost at $ 390,752. It is clear that the continuous expansion of the IOT ecosystem means more possible access points and weak areas need to be reduced.

According to a report by the British certification agency Crest on cyber security in the environment of industrial control systems (ICS), which are a major part of the IoT, the weaknesses that can compromise their work and thus the overall functioning of critical national infrastructure (CNI) are:

- Unauthorized communication protocols

- Outdated and outdated hardware
- Weaknesses in user authentication
- Weaknesses in file structure integrity checks
- Vulnerable operating systems
- Undocumented relations with third parties - interventions of unauthorized specialists.

One of the main findings of the report is the lack of periodic, standards-based, technical safety tests, which are common in many other industries. Therefore, owners and operators of ICS environments do not have an objective way to understand whether cyber risk is adequately managed, so companies and consumers need to be prepared for the many problems that the mass penetration of IoT will pose.

4. Main risks and measures to prevent hazards.

4.1 Hardware and software on a modular basis.

One of the main dangers of recent years is rapidly targeting the ransomware, developing a special tension designed for control systems, propulsion vehicles, assembly lines and energy systems. It blocks the boot area of the operating system, making the device unusable without the ability to restore from backup or until the owner decides to pay ransom, the latest example - Petya. Suspension can cause financial loss, environmental impact, or loss of life. For example, last year alone, 63% of businesses reported that ransomware attacks led to downtime. This forty five percent indicate that it causes hardware damage or data loss. This requires a modular structure in the network with the available IOT, separating these devices in its own network segment or vlan, by rating them into a rapid response with subsequent replacement of failed elements.

4.2 Reduce IoT vulnerabilities and prioritize

Because most of IOT devices require a firmware update to protect us from weaknesses, it may not always be possible in the presence of a large number of IOT (and separate). A patch on a particular device often requires additional time and effort, unlike a normal server, workstation or regular desktop system. Another challenge is default credentials that are provided when internet devices are first used. Often the device, such as wireless access points or printers, is known as the administrator ID and password. In addition, devices can provide an embedded web server, in which the administrators can connect remotely, log in and manage the device. It is a large vulnerability that can put IOT devices in the hands of hackers. This requires companies to develop strict rules in the commissioning process. This also requires them to create a growth environment in which the initial device configuration settings can be tested, which can be scanned to identify any weaknesses, and then valid and "off". Before the device is placed in the actual production environment. Further compliance team needs to verify that the device is ready for production, time -time to test security and to ensure that all changes are closely monitored, controlled and login operational weaknesses are logged and competent authorities are addressed.

4.3 Rapid identification of potential threats by analyzing traffic and placing controls in appropriate places

The variety of new devices with wireless Internet access will create a stream of data for businesses to collect, summarize, process and analyze. Although this opens up new business opportunities, new risks also arise. This requires rapid identification of legitimate or malicious traffic patterns on IoT devices. A simple download of a seemingly legitimate application of a consumer smartphone that contains malware should be identified and accessed. Analytical tools and algorithms must detect malicious activity,

stopping the spread in the network, especially to points with IoT, which would lead to the collapse of subsystems and control modules.

4.4 Proper understanding of the complexity of possible vulnerabilities

Every day, unknown hackers hack in popular sites and portals, social networks, blogs and forums. This only indicates at high risks that IOT devices will pose to companies and general users. If a nuclear power plants are successful in manipulating a casual hacked reading of IOTs attached to some sensors and the device is compromised, the results may be the same for a natural disaster. Understanding where the weaknesses of a particular tool are and how serious they are threatened that they will become a major dilemma. To reduce the risk, any project associated with data transmission devices must be designed for safety reasons. As these devices will have hardware, platforms and software that the company has not used earlier, requiring a very careful evaluation when designing the new network structure. It is important that the risk produced by many internetconnected devices is not deemed to be less.

4.5 Attempts to disintegrate systems and DDoS (denial of service) attacks

Ensuring continuous operation of internet-based equipment would be important to avoid potential operating failures and blockage of corporate services. Even a network appears to add new endpoints - especially automated machine -to -masheen communication equipment, such as those who help start power plants or monitor environmental control - will require businesses to focus on possible attacks on equipment in remote places. This will require businesses to increase physical security to prevent unauthorized access to equipment outside the security perimeter. Destructive cyber attacks, such as widespread denying of broad service (DDOS) attacks, can have harmful effects on an enterprise. If thousands of such IOT devices try to reach a corporate website or information system of a large company, their customers will be disappointed, which will cause revenue, consumer dissatisfaction and loss of market and image. Many challenges facing IOT are similar to byod (bringing their own devices) - individual laptops, tablets, smartphones used in the workplace. The ability to manage lost or stolen tools - eradicating important data from a distance or at least disable its connectivity - would be important to deal with compromised equipment. This will help reduce the risks associated with corporate data that can fall into criminal hands. Other techniques that help manage byod can also be useful - encrypting important data, password access, etc.

5. Protection planning

The above threats and the measures related to them require the mandatory development of a protection plan for all IoT system users. Each layer of defense requires different security measures. For example, phishing awareness training will teach users not to click on malicious links in emails. The layers should include:

- Physical access. Biometrics, security guards and locked doors.
- Perimeter. Demilitarized zone, firewall and VPNs.
- Internal network. Protected with a network-based intrusion detection system and intrusion prevention system, network segmentation, network access control, and network-based antivirus protection.
- Host. Harden the host with the latest patches and blocking services that shouldn't be exposed by doing port control, host-based antivirus protection.
- Application. Conduct input validation and follow best practices to protect applications, harden the application, and have access control and authentication for applications.

- Data. Encrypt data, prevent data loss or leakage, and have backups for data. Always test the data backups.

6. Conclusions

One of the directions in the development of digital technologies is the increasing penetration of IOT. This vast capacity will require better and better means and methods of safety, given its quantitative growth. A smooth infection from traditional cyber security requires a smooth infection, including individual computers, servers, mobile devices, and traditional IT infrastructure, the risk for the protection of a wider range of management and interconnected devices, sensors and technologies, the number of which is also uncomfortable in the near future. Responsibility and challenge for the IT sector, which must study good safety practices and ensure that IOT works properly in corporate networks related to communication, data collection, process monitoring and many other applications. This increased complexity should not be ignored, and modeling and increasing security of potential threats will ensure the privacy, integrity and access of any system in the digital world associated with this rapid difference.

References:

1. M.Rouse, https://internetofthingsagenda. Tech target .com / definition/Internet-of-ThingsIoT? src=6305273 &asrc= EM_ ERU _130530409& utm_medium =EM& utm _source =ERU& utm_campaign= 20200703 _ERU% 20Transmission %20for%2007/ 03/2020%20 (UserUniverse:% 20307418) &utm_ content=eru-rd2-rcpB, Accessed July ,2020.
2. L.Rosencrance, https://internetofthingsagenda. Techtarget.com/tip/IoT-network-architecture-shaped -by-businessrequirements Accessed May, 2020.
3. K.Gloss, https://internetofthingsagenda. Tech target.com /tip /Tackle-ICS-IoT-security-challenges -with-6- processes?track=NL1843&ad=934659&src= 934659 &asrc= EM_NLN_ 129937235 & utm_ medium=EM& utm_source=NLN&utm_ campaign =20 00623_ Tackle %20ICS %20IoT%20 security %20 challenges%20 with %20 processes Accessed Jun 2020.
4. International Journal of Scientific & Engineering Research Volume 11, Issue 8, August-2020 1070 ISSN 2229-5518 IJSER http://www.ijser.org Author: Hristo D. Panayotov PhD Dept. of Information Technologies , Assen Zlatarov University, Burgas - 8000, Bulgaria.