Tackle IoT security challenges - risks and measures to prevent hazards

Hristo D. Panayotov PhD

Abstract: This article discusses trends in IoT development and the problems associated with ensuring their functionality in an environment of increasing cyber threats to such systems. Their wide use in industry, services and other areas, incl. administration, increases the risks of unauthorized access to the resources of various local and corporate networks, as well as desktops, web servers, databases, etc. The article is an attempt to systematize and summarize the methods of risk analysis, as well as ways to prevent them. Recent developments in IoT hacking practices, such as ransomware, DDoS, botnets and others, have also been reported. The issue is focusing on how to prevent compromising and often degradation of whole production units, as well as elements or entire infrastructural systems.

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

1 Introduction

Why is IoT becoming more popular? Owning and using them creates new opportunities and gives an advantage to both the average consumer and the business. This creates huge opportunities for businesses to develop new services and products, creating incredible conveniences and even greater satisfaction for their customers. Initially focused on the requirements of the individual user, at present the application of IoT in business is beginning to exceed even our wildest dreams. For example, chipped shipments that, when connected to the recipient's local network, automatically update its logistics systems. In IoT medicine, sensors are connected to the patient, showing real-time data on basic vital functions and allowing remote action. In short - the possibilities for use are unlimited, as well as the number of devices that can be connected. But although the connected ecosystem is quite expansive in 2019, it is set to grow even more in the coming years. We are at the peak of an era when almost everything around us has some form of internet capabilities, such as home appliances, cars, office equipment, urban infrastructure and healthcare devices.

For many, the Internet of Things (IoT) will mark the next great revolution for humanity. According to Statista, 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-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for instance, to set them up, give them instructions or access the data.[1]

Looking inside there are six IoT network architecture components: [2]

- 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.
- 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 potential of IoT, there are many risks that need

to be considered when building such infrastructures. Because these are devices designed to connect to the Web, their operating system is built into their firmware. Precisely because of this fact, these embedded operating systems are not designed with antivirus protection as a priority and paramount consideration, which is why their vulnerability to cyberattacks is present in almost all of them. The most recent example is the avalanche of malware targeting Android-based devices. Similar threats are likely to spread to the IoT as soon as they log in to any network. Along with the dangers in the Edge layer (sensors, actuators, devices), the classic attacks in the communication segment and that of the application software - viruses, phishing, botnet, theft and data destruction - are increasing. Hackers are using connected devices to collect sensitive data, send spam, monitor networks and launch cyber attacks around the world. Botnet attacks have become commonplace, with the CenturyLink Threat Research Lab estimating that 195,000 such attacks take place each day, and Accenture setting the average cost at $ 390,752. It is clear that the continued expansion of the IoT ecosystem means more potential access points and weak areas that need to be mitigated.

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 Building IoT hardware and software on a modular basis.

One of the main threats of recent years ransomware is increasingly targeting the IoT, developing a special strain designed for control systems, propulsion vehicles, assembly lines and energy systems. It blocks the boot area of the operating system, making the devices unusable without the ability to restore them from backups or until the owner decides to pay the ransom, the latest example - Petya. Suspension can lead to financial losses, environmental impact or even loss of life. For example, last year alone, 63% of businesses reported that ransomware attacks led to downtime. Forty-eight percent indicate that this results in hardware damage or data loss. This requires a modular structure in the network with available IoT to have a rapid response by isolating these devices in their own network segment or vLAN, with subsequent replacement of failed elements.

4.2 Reduce IoT vulnerabilities and prioritize them

Because most IoT devices require a firmware update to protect against vulnerabilities, this may not always be possible in the presence of a large number (and different) of IoT. A patch on a particular device often requires extra time and effort, unlike a normal server, workstation, or regular desktop system. Another challenge is the default credentials that are provided when Internet devices are used for the first time. Often devices, such as wireless access points or printers, have known administrator IDs and passwords. In addition, devices can provide an embedded Web server to which administrators can remotely connect, log in, and manage the device. This is a huge vulnerability that could put IoT devices in the hands of hackers. This requires companies to develop strict rules in the commissioning process. It also requires them to create a development environment in which the initial device configuration settings can be tested, scanned to identify any vulnerabilities that may occur, and then validated and "closed". before the device is placed in a real production environment. This further requires the compliance team to verify that the device is ready for production, to periodically test security and to ensure that all changes are closely monitored, controlled and logged operational vulnerabilities are logged and addressed to competent authorities.

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 into popular sites and portals, social networks, blogs and forums. This only hints at the high risks that IoT devices would pose to companies and ordinary users. If a seemingly accidental hack of IoT connected to certain sensors at a nuclear power plant

succeeds in manipulating the readings and the device is compromised, the consequences could be tantamount to a natural disaster. Understanding where the vulnerabilities of a particular device are and how serious a threat they pose will become a huge dilemma. To reduce the risk, any project involving data transmission devices must be designed for security reasons. As these devices will have hardware, platforms and software that the company has not used before, this requires a very careful assessment when designing the new network structure. It is crucial not to underestimate the increased risk posed by many Internet-connected devices.

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

Ensuring the continuous operation of Internet-based devices will be important to avoid possible operational failures and interruptions to corporate services. Even the seemingly simple process of adding new endpoints to a network - especially automated machine-to-machine communication devices, such as those that help start power plants or monitor environmental controls - will require businesses to focus on possible attacks on devices in remote locations. This will require businesses to increase physical security to prevent unauthorized access to devices outside the security perimeter. Destructive cyberattacks, such as widespread denial of service (DDoS) attacks, can have detrimental effects on an enterprise. If thousands of such IoT devices try to access a corporate website or information system of a large company, their customers will be disappointed, which will lead to loss of revenue, consumer dissatisfaction and potential deterioration of the market and image. Many of the challenges facing IoT are similar to those of BYOD (Bring Your Own Device) - personal laptops, tablets, smartphones, used in the workplace. The ability to manage lost or stolen devices - remotely erasing important data or at least disabling its connectivity - will be crucial to dealing with compromised devices. This will help reduce the risks associated with corporate data that could 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: [3]

- 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 Conclusion

One of the directions in the evolution of digital technologies is the increasing penetration of IoT. This huge potential will require better and better means and methods of protection, given its quantitative increase. A smooth transition is needed from conventional cybersecurity, involving personal computers, servers, mobile devices and traditional IT infrastructure, to risk management and protection of a much wider range of interconnected devices, sensors and technologies, the number of which is unpredictable even in the near future. Responsibility and challenge to the IT sector, which must study good security practices and ensure that IoTs work properly in corporate networks related to communications, data collection, process monitoring and many other applications. This increased complexity should not be overlooked, and modeling potential threats and increasing security would ensure the confidentiality, integrity and accessibility of any system in this increasingly inter connected digital world.

References:

[1]
M.Rouse,https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT?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-business-requirements Accessed May, 2020
[3]
K.Gloss,https://internetofthingsagenda.techtarget.com/tip/Tackle-ICS-IoT-security-challenges-with-6-processes?track=NL-1843&ad=934659&src=934659&asrc=EM_NLN_129937235&utm_medium=EM&utm_source=NLN&utm_campaign=20200623_Tackle%20ICS%20IoT%20security%20challenges%20with%206%20processes Accessed Jun 2020

Author: Hristo D. Panayotov PhD
Dept. of Information Technologies , Assen Zlatarov University, Burgas - 8000, Bulgaria e-mail: itko59@gmail.com