

IoT SECURITY PROJECT

Katarzyna Badio 145306



1. IoT devices in medicine.

Medicine in IT has had many advancements in the recent years. With this fact, it is clear that also some new vulnerabilities have been discovered. Every year we can hear from the media that an attack occurred on some healthcare company and data of the patients has leaked. Medicine in IT is very broad field, AI in medicine has been trending, but also IoT devices play important role in healthcare. There is very wide range of devices, from small ones to large systems, which are crucial in curing patients.

There are many ways of classification of medical devices, but I will focus on the functionality they provide. The first class of IoT in healthcare are ,,remote patient monitoring systems’’ (RPM) [1] which are systems that monitor patients health parameters. As mentioned in a webpage “health recovery” there are devices from this class that measure blood pressure, holter [3], glucose level in blood [2]. There is also a device such as pulse oximeter, that tell what is the level of oxygen in the blood [2], one of the most important parameters in determining overall health of the patient. Another popular device are ECG and Stethoscope [2]. Some wearables also have some of the functions like the devices mentioned above. With these, it is possible to measure blood pressure, glucose, heart rate and oxygen level [2].

According to Babirus [3], some other types of machines are ,, diagnostic medical equipment, treatment medical equipment, medical imaging machines and laboratory equipment in Medicine’’.

Laboratory devices consists of ,,microscopes, centrifuges and spectrophotometers’’ as mentioned in Babirus [3].

Treatment equipment class has many more devices, such as ,,surgical lasers, infusion pomps, ventilators, dialysis machines and defibrillators” [3].

Some more advanced devices are surgical instruments and MRI scanners.

I will focus on wearables IoT devices in different fields of medicine.

1. Details about group of devices

Usually IoT devices come together with the applications on smartphone, which ensures that the person is feeling the best he/she can [3].

The most important characteristics of the IoT system is connectivity, which helps to make links with the infrastructure [4]. Without it a IoT device would be useless, it must connect fast and be accessible easily. Some another thing is that IoT market is growing very fast, so that in each home there is more and more devices which form a network together, so the system must be scalable [4].

According to Oroos Arshi, Aryan Chaudhary [4], there are five layers of an architecture of IoT system. First, is the Edge Technology Layer which includes hardware and sensors, for example, all of the components which the device is made of. Next, is the Access Gateway Layer which connects the device with the client side. Internet Layer is crucial in interaction between two end points. There is also middleware layer and application layer.

1. Communication with the group of devices
2. Overview of the security issues

Example issues are taking photos while being hidden and collecting data from random people all around without their knowledge [3]. Some devices with this functionality are sold only to the companies instead of all people, to prevent such issues [3].

Another problem is that devices can be wrongly encrypted, which was mentioned also by S.Babar, A.Stango, N.Prasad [5], there is a vulnerability that there are clear-text credentials which can be unencrypted.

S.Babar, A.Stango, N.Prasad classified issues by attack surface areas. Some of these issues are popular among web applications, like SQL injection, Cross-Site-Scripting, Cross-site request forgery and not that popular as the other ones, username enumeration. The last one is when the threat actor brute-forces a user credentials and tries to guess them based on the server’s response to the invalid ones [6]. A person also must take care of weak passwords and default credentials which are often not changed within IoT devices, such as “admin” or “root”.

Some more interesting vulnerabilities include taking control of a device using third party credentials [5]. A person should regularly review which programs have access to the wearable. People are usually allowing access on default and can be later surprised that so many devices have access to personal data. That is then more difficult to manage and detect attack, which could come from many sides. Also there are privacy concerns about the data being stored [5].

1. Analysis of vulnerabilities in the device
2. Defense from the vulnerabilities
3. Overall

[1] <https://ordr.net/article/iot-healthcare-examples>

[2] <https://www.healthrecoverysolutions.com/blog/7-common-remote-patient-monitoring-devices>

[3] <https://www.deepseadev.com/en/blog/wearables-and-iot/>

[4] Fortifying the Internet of Things: A Comprehensive Security Review, Oroos Arshi, Aryan Chaudhary

[5] Conference: S.Babar, A.Stango, N.Prasad, J.Sen and R.Prasad “Proposed embedded security framework for Internet of Things”.

[6] https://www.rapid7.com/blog/post/2017/06/15/about-user-enumeration/