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.

2. 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][7]. It is also important to note that IoT devices are made of many parts, which makes them heterogeneous objects [7]. Also, IoT devices produce a lots of data because of sensors [7].

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, 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.

For example, there is a group of wearable devices used in psychiatric research, such as ,,wristwear, clothing, belts and body patches, containing sensors to measure psychical activity. The sensor data from the wearables may be combined with other data sources, and used to classify emotional reactions, mood states and stress in various psychiatric disorders'' [8].

Another example listed in [10] of IoT devices, which can be worn on a body are, Wearable Fitness Trackers, such as Fitbit, Jawbone and Polar loop. Another category of devices is Wearable ECG Monitors, such as Fitbit sense, Fitbit Versa 3. Some other are Wearable Blood Pressure Monitors, examples of these devices are BPM Connect and Omron platinum. I will later analyze security issues within the FitBit wearables, especially FitBit One and Fitbit Flex. FitBit clock measures "user step counts, distance travelled, calories burned, floors climbed, active minutes, and sleep duration" [11]

3. 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. This is also mentioned in [10].

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].

Another issue is that IoT devices don't have normal operating systems and anti-virus software, have not good software update systems [9].

4. Communication with the Fitbit devices

Fitbit uses BLE Protocol (Bluetooth Low Energy Protocol) [11]. This protocol is really important if a user wants to have low power rather than high throughput [12]. This kind of communication is useful when a device must be on for short amount of time and then can go to sleep mode.

There are two main types of messages sent by the tracker, microdumps and megadumps as observed by the team [11]. The app makes HTTPS requests based for authentication. "Each basic action is accompanied by a so-called microdump, which is required to identify a tracker and to obtain its state". It is sent in plain text.

Megadump contains of more data, such as steps count [11]. The megadump is sent to the server and then reply is sent to the tracker. A megadump contains a header, one or more data sections and a footer. Data sections contain statistics such as Daily summary, Per-minute Summary, Overall Summary [11].

5. Analysis of vulnerabilities in the Fitbit device

According to the publication [11], Fitbit is one of the most secure intelligent watches. However, it is possible to exploit these devices by reverse engineering the communication between them and cloud and “extract sensitive information in human-readable format” by using open-source tool [11]. It is also possible to “inject prefabricated activity records to obtain personal benefits” [11].

Researchers in [11] has created MITM proxy, which acts as a wireless Internet gateway, there is fake CA certificate installed on a phone. Then, the tracker functionality is manually run and synchronized with Bluetooth with the application. Next, the data is sent to the Tracker Remote Server over Wi-Fi. MITM allows to intercepts all requests, because there is no end-to-end encryption.

While microdumps and megadumps were mentioned in this report, more information will be provided in this section. Plain-text messages are validated by CRC-CCITT checksum, to detect data corruption by the server [11]. This knowledge enables the researchers to inject messages and get replies, such as checking if the ID of a tracker is valid and has a user account.

It is possible to construct megadump manually, send it to the server and update Fitbit information. What is important to note, that only user ID must be known, without the tracker itself, to modify data. To create a message, a Fitbit frame must be Base64 encoded and placed in XML code [11]. The issue is that if it is possible to upload to any ID, there is possibility for DoS attack. CRC was unknown for the unencrypted packets, but if the message was sent with the wrong CRC, then the server responded with correct CRC, so it was possible to fix it and send again the request.

6. Defense from the vulnerabilities

In the paper [4], some solutions to the IoT vulnerabilities were proposed. I will list some of them and give some explanation. First one is “Identifying and controlling devices”, which means that every IoT device must have ID number assigned to it so it’s distinguishable from the other devices in easy way. Also Trustworthy Platform Modules should be used, because they enable securing storage of a key. Another important thing is “Mutual Authentication”, so that server and a client exchange certificates with handshake process. Authentication should be through certificates provided by the CA, and should be two-factor, because “it adds extra degree of protection”.

There should also be a system which actively monitors the device and looks for anomalies (“Continuous Monitoring”) [4]. Also, Role-Based Access Control should be provided. Last thing I want to mention is “Zero-Touch Provisioning”, which “enables devices to automatically get their credentials and securely join to a network”.

7. Overall

The text provides an overview of IoT devices in medicine, focusing on their functionality, security issues, and potential vulnerabilities, especially in wearable devices like Fitbit. It highlights the architectural layers of IoT systems and examples of exploitation. Solutions such as mutual authentication, continuous monitoring, and zero-touch provisioning are proposed to mitigate these vulnerabilities and improve device security.

[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/
[7] Security Issues in using IoT enabled devices and their impact; Vishal Dineshkumar Soni
[8] Internet of things issues related to psychiatry; Scott Monteith, Tasha Glenn, John Geddes, Emanuel Severus, Peter C. Whybrow and Michael Bauer
https://creativecommons.org/licenses/by/4.0/
[9] IoT Cybersecurity Alliance 2017; Bacelli et al. 2013
[10] Security Risks and User Perception towards Adopting Wearable Internet of Medical Things; Sanjit Thapa, Abubakar Bello, Alana Maurushat and Farnaz Farid
[11] Breaking Fitness Records without Moving: Reverse Engineering and Spoofing FitBit; Hossein Fereidooni, Jiska Classen, Tom Spink, Paul Patras, Markus, Miettinen, Ahmad-Reza Sadeghi, Matthias Hollick, Mauro Conti
[12] https://novelbits.io/bluetooth-low-energy-ble-complete-guide/