CYBER SPS

CYBER SECURITY PROFESSIONAL SOLUTIONS

IoT Security Risks in Healthcare Systems

Report

August 2021

Email: kontakt@cybersps.de
Telefon: +49(0)5371 9 370 672

https://cybersps.de
USt-IdNr.: DE336337314 Finanzamt Gifhorn

Bei GWM GmbH, Am Mühlengraben 22
38440, Wolfsburg

Internet of things (IoT) that includes anything that can connect to internet and together such as smart phones, vehicles, smart watch, smart TV, health tracker sensors, smoke detector sensors, etc. is going to get more foot on our everydays' life and we are somehow getting dependent to these technologies, as they enhance our lives.

The COVID 19 also increased the use of IoT functioning by helping to provide the same services without any contact or touch. Some examples are Corona Warn application to detect the areas where infected peoples are or to make a possibility to inform all people who were in contact with a COVID 19 positive cases.

Another example is providing the COVID19 Vaccine required maintenance such as required temperatures, humidity, etc. That the vaccine keeps its good condition.

Automatic Hand Hygiene reminder is another IoT sensors that remind the patients and hospital staff to sanitize .

The IoT made it also possible for the doctors to remotely monitor the status of their patients via different health tracking sensors. e.g. The sensors that collect the patient heart pulse or blood sugar or other health behavior of the patients and send it directly to hospital for further analysis or alarm the doctors over the abnormally of the collected data. Some examples of these IoT devices are the followings:

- ADAMM: an asthma monitoring health device
- Glucose monitoring: for the patients with positive diabetes
- Parkinson disease monitoring by providing all symptoms of patients to doctors
- Depression monitoring: IoT devices with the help of Artificial intelligent (AI) can detect the depression symptoms and panic symptoms on patients and can involve the related health care system for possible treatments.
- In Hospitals there are also possibilities and there are existing devices that are used to regularly give patients their required dose of medicines. This is usually configured by the doctors or specialist and the device will inject the doses to patient in the given time through connected serum on patients.
- MRI systems is used to diagnostic different tissue of the body.
- Pacemakers are a small piece placed under the skin in chest to control the hearthbeat to be more regular and help the heart to react normally.

and it is coming more such as remote surgery of patients by entering small robots in patients body and via them doing very complex surgeries.

Although, technologies such as IoT is very attractive, nevertheless, having more and more connected devices to internet and together increase the chances and open doors to criminal attackers to misuse those systems which may lead potentially dangerous situation, especially if the sensors are having critical functionality.

Usually IoT devices are using one of the following connection methods

- Bluetooth: the attack can happen via hacking the bluetooth software, by finding the vulnerabilities or use the known vulnerabilities, if the software is not up to date.

- WiFi: similar to bluetooth, the attacker can target the Wifi driver software.

- Mobile networks: there are alreay known vulnerabilities in mobile networks that allows the attacker to be MITM communication. This is because the 3GPP standards because of handling disaster situation such as earthquick, flooding, etc. allows such situation.

- Internet cables: the attack can happen via hacking one of the computers in the named network and via this victim computer, try to hack other devices.

- NFC/RFID: the attacker needs to be near the device or hack the receiver of the IoT information and manipulate the IoT device via this receiver. Like sending false information.

The attacks on Health care IoT system can be result in two different situations:

1. **Information expose: the attack will cause the patient information to be accessible publicly on internet.**

One example is the misuse of Corona Warn app communication method. Corona Warn app can receive information about the other nearby mobile phones via constantly advertising an identity using Bluetooth signals. For this purpose the bluetooth interface shall be active in the mobile phone. What we as user see in bluetooth is only the application layers as stated in figure 1 as very high level architecture of bluetooth. The bluetooth stack includes any drivers that needs to run the hardware and convert the application messages to hardware based required language. There were a lot of known vulnerabilities in bluetooth stack or applications that allow attacker to take control of the bluetooth enabled device, such as a smart phone. The attacker might be able to install a backdoor on the mobile phone of the victim after taking control over it. This will result in accessing many personal information of the user such as bank information, Corona status, home address, name and phone number, his/her contacts information, etc. that the information can be used for spoofing and misuse.

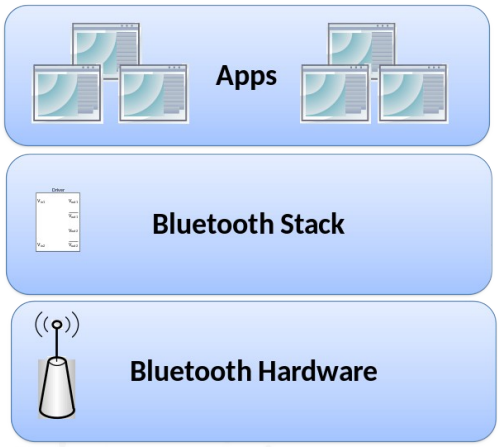

Figure 1. very high level overview of Bluetooth architecture

2. Information manipulation and safety risks

The attacker not only takes control of the IoT device such as health monitoring sensors, but also sends false information, that may result in injury or death of a person.

Some examples are as following:

- The attacker hacks the device that gives required medicine doses to patient via Wifi connection or bluetooth connection that the device has and overdose the related medicine. This may result in damaging any critical organs such as Heart, Kidney, Brain, Liver, etc. or may result in the patient to be in Coma.
- If the hospital network is hacked and via that an Xray remote control system is hacked, during the xray, sends more radiation than necessary which may cause cancer or death.
- MRI Systems providing the information using magnets. Hacking MRI Systems may result in high magnetic environment, that will have a negative impact on nerve systems and biological aspects of bodies.
- Manipulating the pace makers will cause the pumping to be so fast which causes disorders in patients.

Therefore, preventing the attacks and securing Health care IoT sensors and devices are important, which plays a high role in death or injury prevention of patients.

There are some possible protection mechanism to secure the IoT devices against attacks. Some general examples are as followings:

Security mechanism	Advantages	Disadvantages
Transport layer security (TLS) : a security standard protocol	- for instance instead of using http, the use of https - the message is encrypted during transport and not readable (see	- the IoT Sensors might not support https, because of needed resources - the IoT sensors which has Hardware Security Module (HSM) or an storage to

	figure 2) - it provide also authentication. In other word, to verify the identity of the sender or receiver	store the secrets or private keys can be very expensive and not very cost effective - For real time sensors, the encryption might cause delays
Anomaly detection systems	The use of any Intrusion detection and prevention systems (IDS) to detect any malicious behavior in the network that the IoT sensors are connected	- It might be the case that not all malicious activities is detected - Using such systems need also professional IT expert people for maintenance
Physical protection: Keep the sensors and IoT devices out of the reach that are not physically accessible or use security cameras to check the access	- Usually IoT sensors are not protected against the attacker who has physical access to them. This will help to protect the device from installation of malicious software such as malware, virus, randsomware, etc. Directly on the device	- It is not possible to protect all sensors or IoT devices. e.g. MRI systems are still placed where attacker can go to that room or access them, even as a patients.
Encryption of the data storage	- if the device is being stolen, the attacker cannot read the confidiential data	- if the keys for encryption is not good protected or is inside the device, it might be still possible for the attacker to read out the key from the device and decrypt all messages inside
Penetration testing and system audit	This will help to detect any flaws on the IoT device or in general, depends on the scope, on the systems, where IoT devices are used	- It can be time consuming - Implementation of the security measures after vulnerability findings can be costly - it needs experts to do this who has experiences
Training Staff	- Awareness of how the attacker can attack the system and avoid any easy way of attacking, will help to decrease the possible attacks	- It might be costly - It needs time
Keeping the IoT systems up-to-date	- This will disallow the attacker to use the known vulnerabilities in IoT systems to easier take control over them	- it might cause compatibility problems of the device with other devices - the IoT device might not support the remote update and then it needs to be updated one by one by experts, which is

time consuming and costly

- The provided patch for a zero-day vulnerability might be available so late, and during this time, the device is still exposed to the attacker.

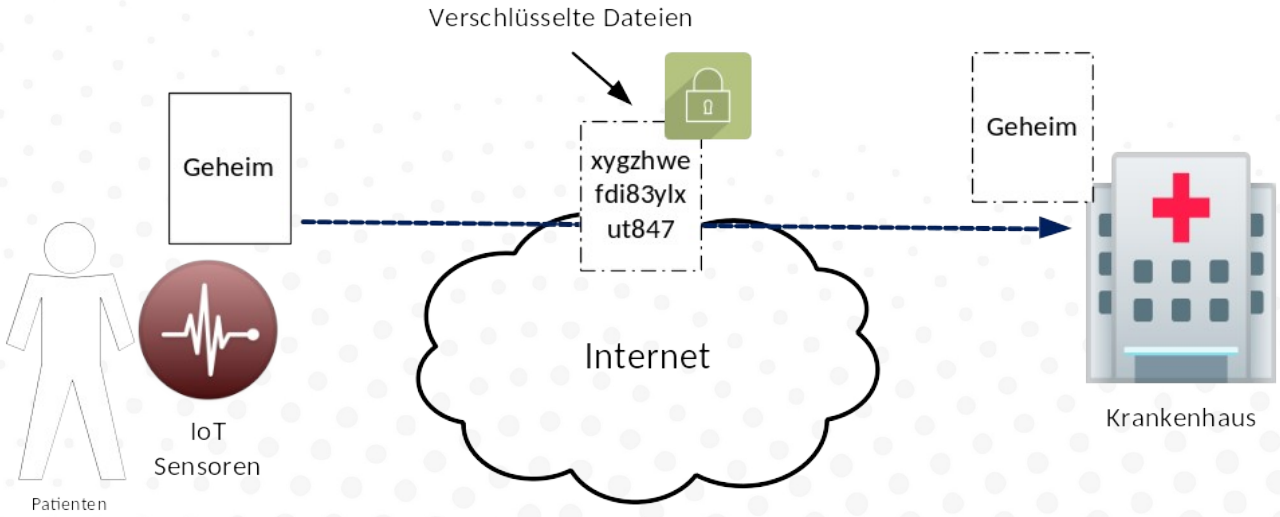

Figure 2: it shows the protection of IoT datas via encryption during transport

Although, there are some security mechanism as explained above, but security is not 100% and those security mechanisms try to minimize the risks to the extend that can be acceptable and the risks can be handled. Further, human error constitute the major security risks in any systems, including IoT. For instance, failure in secure configuration of the IoT devices which allow that attacker to take control over the device. Another example is failure during developing of the software for IoT device, that may result in further flaws to be introduced to the device and allow the attacker to exploit these flaws and easier take over the IoT device.

Therefore, it is necessary to do regular risk assessment for the assets (e.g. IoT sensors, health care place IT network, etc.) in health care systems and keep track of any changes in systems. Because the changes might be small but the security risks might be high.

Further, all the health care companies and health care organisations need to be prepare for any possible incidents that might happen during the lifetime of any IoT- device in use by their place. In other word, an incident response team is needed to be prepared for a fast reaction of any reported 0-day vulnerabilities. If the health care place does not have themselves the necessary expertise, they need to look for expertise in this area to support them. Although, one major problem in some of the health care organisations is that, they usually assign very limited resources for securing their systems, until the flaws is exploited by a criminal attacker, then it is too late and the flaws might caused safety risks or exposure of patients' data.

CyberSPS team can provide the health care places necessary security risk assessment ,testing and also help them to build their security teams by providing the necessary training for their staff in order to minimize the security risks, especially, caused by human errors as stated above (e.g. misconfiguration).

CyberSPS is also ready to support the governments and EU commission to enacting necessary regulation to protect the IoT systems in health care systems by providing the vast experiences in this area.

Autor:

Dr. Hosnieh (Sara) Rafiee

She is the cyber Security expert by CyberSPS.de, where offer penetration testing for IoT and IT systems, training and further consultant to secure all systems in health care places.

She has done her PhD in the area of Security in Internet technologies by Hasso Plattner Institute. She has more than 15 years of experiences in completely different security areas that includes: Automotive, IT, Cloud, 5G Network security, SDN, NFV, IoT. She has also valuable experiences in standardisation such as ETSI, IETF, IEEE, ISO 27000, BSI, PCI DSS, and EU Data protection. She worked for different companies and organisation as contractual or employee such as VW, Huawei, SAP, etc. She has also "International Professional Teaching" certification and till now has provided some trainings in the area of penetration testing, security awareness and programming languages such as C, C++ and C#. More details can be found on her Linkedin profile or on her private website (please click here).