Safety Issues of Implantable Medical Devices

Xiangyu Gao

1. A summary of the evaluated technology.

An implantable medical device is one that is placed inside your body during a medical procedure and is intended to stay there after the procedure.According to the FDA's definition, an active medical device is "a medical device that relies on electrical energy or an energy source not directly generated by the human body or gravity to perform its function." Active implantable medical devices are "medical devices intended to be inserted into the human body in whole or in part by surgical or medical means or by medical intervention into the body's natural orifices and retained after surgery". The device has many applications, such as implantable cardioverter defibrillators (ICDs) or implantable sleep apnea devices for the treatment of disease. With the capabilities of data collection, wireless connection and near-field communication, it can not only monitor various health indicators of the human body but also cure diseases and restore human function.

In recent years, a new generation of implantable electronic medical devices has gradually replaced traditional wearable medical devices and has become a hot spot in global medical research and development. Compared with traditional portable electronic medical devices, implantable medical devices are more convenient, faster and more accurate. It has functions such as data acquisition, wireless connection and near-field communication. It can not only monitor various health indicators of the human body but also treat diseases and restore human function.[1]

2. Assets, and privacy and security goals.

First, implantable medical devices are used to do things that conventional surgery cannot. Such as some types of deafness, and some special heart diseases.They enable people to gain a sense of well-being in life by making it easier for people to perform specific functions. They can not only monitor various human health indicators, but also treat diseases and repair human functions, such as seeing better, hearing better, and even maintaining The heart beats normally.

Then, a very important task of this type of equipment is to prevent it from being controlled by outsiders. Some devices may not kill you, but if the medical devices that sustain your life can be easily controlled by others, the consequences are unimaginable - that is, your life is between other people's fingers. To encrypt the device with any useful encryption including hardware method encryption or algorithmic encryption.

3. Potential adversaries and threats.

User data can easily be compromised. Some implantable medical devices are not strictly regulated by law, so most of those medical tech companies are self-restraining. Moreover, the user's information is easily collected by the company, and there is a certain risk of being stolen or even used for commercial purposes.

Some agents from hostile countries. If people in a hostile country want to access some of their data, such as some classified map data, then they can use some devices such as fitness trackers to use the GPS on them to obtain such classified data. Or if they want to eavesdrop on confidential conversations, there is a chance that hearing aids could be used to eavesdrop.

4. Potential weaknesses.

First, if an implanted medical device were to be hacked, the patient's life would be an imminent threat. For example, a remote attacker could install malware to control a pacemaker, causing it to kill the heart or refuse to work if necessary to save a patient's life. If an attacker hacked into a diabetic's insulin pump, they could remotely control the dose of the drug, turning it into a lethal dose.

Additionally, pacemakers, insulin pumps, hearing implants, and other readily exploitable IMDs may leak GPS and location data, as well as other potentially classified datasets or environmental information related to safe rooms that are built-in Sensors, microphones, etc. Sensors that convert environmental information into signals and data. For example, there are smart hearing aids on the market that are linked to cloud architectures and use machine learning (ML) to record and analyze sound for feedback and improve its performance, but if compromised, this functionality could be abused.[2]

Third, unlike desktop computers and servers, this category of IoT devices cannot run antivirus software and other endpoint data security checks. Their diversity, and their disregard for their safety in the first place, often make them impossible to compromise. In one currently used attack method, known as MedJack, attackers inject malware into medical devices and then spread it across the network. Medical data found in these types of attacks can be used for tax fraud or identity theft, and can even be used to track drug prescriptions, enabling hackers to order drugs online and then sell them on the Dark Web.[3]

Privacy breaches are also an important topic for citizens and users. No one wants their information to be used for sale or other bad purposes without their knowledge. This special medical device becomes a channel for privacy leakage. Because it is difficult for citizens to know if their information is being used by medical companies for other purposes.

5. Potential defenses.

As with other IoT devices, there are two necessary components to improve security. First, medical devices such as watch tables and monitors, which have been on the market for years, require defenses, such as security scans, and simple mechanisms for downloading patches and updates. Going forward, however, future generations of devices also need to be encouraged to provide stronger security protections from the outset. Too many manufacturers ignore security in the early planning stages or simply rely on third-party components that may themselves be vulnerable.

Fortunately, some progress has now been made. The Food and Drug Administration (FDA) began evaluating device cybersecurity more rigorously around 2013 as a criterion for product approval, and this criterion is continually being updated. The FDA's standards are largely based on guidance from the National Institute of Standards and Technology (NIST) on a critical infrastructure cybersecurity framework in 2014. NIST is currently revising the version and has released a separate landmark document detailing the basic approach to developing safe, reliable digital systems. It's not enforceable, but it's a start.

Besides, in 2019, Purdue University engineers further enhanced the safety of networked implantable medical devices with a technique that keeps communication signals inside the body. This private communication network can only be accessed by yourself and your device and is very difficult for others such as hackers to breakthrough. The human body can carry signals very well, and new technology developed at Purdue University can bring the signal very close to the body.

The research team at Purdue University used a method called "Electroquasi-Static Field Human Body

Communication (EQS-HBC)", which confines the signal within the human body by using a low-frequency carrier-free (broadband) transmission method. It makes it difficult for nearby eavesdroppers to intercept key private data, forming a private communication channel, that is, the human body.[4]

Regarding the privacy of citizens, I think it is very necessary to introduce some laws to strictly limit the acquisition and storage of private data of citizens by companies. For example, for the protection of genetic privacy, HIPAA and GINA can provide certain guarantees for the privacy of citizens. For implantable medical devices, each state could also introduce legislation to limit and monitor companies and organizations that may reveal citizens' privacy, thereby improving privacy protections.

6. Conclusion.

I think there is still some real work to be done in this industry. Security is not an optional option, but a necessary and primary concern. Manufacturers should continue to develop, update product security issues, and make some corresponding countermeasures. Even with these measures in place, securing existing equipment and securing new equipment is still a gradual process. At the same time, the healthcare industry as a whole is exposed to threats that implicate innocent patients. There is still a long way to go. Although the ever-evolving technology is constantly updating and iterating on artificial intelligence devices and continuously benefiting mankind, it is undeniable that technology is a double-edged sword that can protect you or attack you. So we have to address this topic that threatens humanity from the root—that is, moral and social issues.

References

[1] https://sterlingmedicaldevices.com/thought-leadership/medical-device-design-industry-blog/what-are-implantable-medical-devices/

[2] https://xw.qq.com/cmsid/20210813A0338Q00

[3] https://36kr.com/coop/toutiao/5066132.html

[4] https://www.purdue.edu/newsroom/releases/2019/Q1/your-body-has-internet--and-now-it-cant-be-hacked.html