Medical Robots and Safety – A Look at Rehabilitation Robots

Marc Ruef
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Abstract: Medical robots are used in rehabilitation and other functions. Constraints in the software are intended to prevent abnormal movements. With networking comes an increase in vulnerabilities, which makes attacks on patients possible. Both manufacturers of devices and clinics must be aware of the risks and learn to deal with them professionally.

Keywords: Cloud, Cybersecurity, Exploit, GSM, Legal, Malware, Market, Penetration Test, Risk, Windows

1. Preface

This paper was written in 2018 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20180614* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

Cybersecurity in the field of medicine [1] is an incredibly complex issue. The sheer volume of equipment now in use means that hospitals, doctors, and patients have become lucrative targets. This article explains why robots used in medical functions need to be considered in this context as well.

3. How does a rehabilitation robot work?

Figure: The exoskeleton

There are various forms of medical robot. One whose futuristic promise has prompted plenty of discussion is the surgical robot. CAS (computer-assisted surgery) makes surgical procedures easier, even automated. This can represent a major increase in the efficiency and safety of operations.

Just as interesting are medical robots that can be deployed for rehabilitation purposes. These devices are designed to assist patients in regaining, supporting, or replacing bodily functions that they have lost.

That includes the “exoskeleton”. This is a device that the patient puts on, or steps into. The exoskeleton envelops the patient, providing assistance with stabilization and movement sequences. Medical exoskeletons are primarily used for disabilities that affect mobility.

This kind of device typically consists of two components. First, there’s the hip and leg struts which support the movement apparatus. This should be light and flexible and as inconspicuous as possible. At the same time, it has to be solid enough to guarantee stability and support. The logistics required for the operation of the exoskeleton are generally stored in a kind of backpack. There you will find the computer elements that enable control – in this case, of the hips and legs.

4. Safety is not the same as security

Figure: Physical safety mechanisms

The most important quality in any medical device is *safety*. Any error in the system or incorrect handling of it should not result in harm to the patient. This is all the more

important in rehabilitation systems, because users are often coping with physical deficiencies that render them fragile and more susceptible to malfunction.

With the exoskeleton, for instance, it is important to ensure that patients can't make movements that would harm them. That means, for example, that the knee can only be stretched to a certain angle. There are various exoskeletons that are used for walking. These may be divided into those that control patients' movements (active) and those that patients can operate themselves (passive).

With active systems, it is all the more important that the mechanisms don't enforce problematic movements. In the software control for these devices, you can configure settings that determine which joints can be moved, on what axis, to what angle, and at what speed. Errors in software-controlled constraints can be painful, or even fatal. By manipulating the device, an attacker could deliberately torture a patient, which might lead to irreparable physical harm.

To reduce this risk, such devices incorporate a physical constraint on movements. This is achieved through simple hinges and stops which must be engaged and can only be decoupled manually. But *as the auto industry has shown* [2], sooner or later time-tested physical mechanisms are discarded in favor of pure digitalization.

5. Architectural problems

Figure: A range of input options

Medical technology follows the usual trends, even when by their nature they run counter to the traditional requirements of medicine. So it is hardly surprising that some manufacturers of medical devices and medical robots are aiming to *cloudify* their functions. There are manufacturers of exoskeletons who fit their devices with GSM modems and synchronize all the data (configuration, patient information, telemetry data) with their cloud.

Leaving aside the *standard criticism of cloud solutions* [3], it is the sensitivity of the data, in particular patient data, which is paramount here. The legislation in a number of countries, including Switzerland, prohibits arbitrary disclosure of patient data. So an exoskeleton that stores such data in the manufacturer's cloud is infringing such laws. But few clinics are aware of this, either at a technical or legal level.

Experience has shown that manufacturers tend to be slow in responding. Cybersecurity in particular is way down their list of priorities. This is partly explained by the fact that the agility required for the necessary safeguards a) cannot be achieved, and b) comes with a great deal of cost and effort. Any adaptation to a device requires new marketing authorization (commonly referred to as certification). The device must in turn be tested for functionality and reliability. There is a reluctance to make this kind of investment in the fiercely contested market of medical technology.

6. External attack possibilities

Figure: Physical connectivity option

Compared to popular software products like Windows and Java, successful attacks on medical devices are relatively rare. But the most likely explanation for this is that there tend to be fewer penetration tests of such devices. And where vulnerabilities are found, manufacturers' lawyers are primarily concerned with using legal channels to prevent disclosure – something we know from our own experience. Nonetheless, vulnerabilities can often be found in medical devices, as we demonstrated in the example of *networked infusion pumps* [4].

And in the end, a medical robot is just a computer. Because they don't usually come with a keyboard and a screen, their exoticism is often considered an advantage from a security standpoint. But most of these devices also come with interfaces that allow communication through such traditional input and output devices. If required, this can occur through a network service, which can be controlled.

The manufacturers of the devices in question are aware of this risk. And they avoid working with specialists, fearing above all that this could reveal major vulnerabilities. And that these could become public knowledge. This state of affairs was common in traditional computer security around 15 years ago. Since then, we have realized that systematic engagement with risks offers a greater advantage.

7. Conclusion

Hopefully the issue of security will be taken as seriously in the field of medical devices and medical robots as the standards applied in the area of safety. But there is a lot of catching up to do. Current and future devices must be checked for vulnerabilities no later than the development phase. And any vulnerabilities identified should be

addressed quickly and definitively. There is no question that this represents a significant investment of time and money. But there must also be no question of countenancing the risk of injury or even death of patients due to malware or exploits.

8. External Links

[1] https://www.scip.ch/en/?labs.20160609
[2] https://www.scip.ch/en/?labs.20180405
[3] https://www.scip.ch/en/?labs.20111110
[4] https://www.scip.ch/en/?news.20170524