Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jörg Sambleben
Erschienen im Magdeburger Institut für Sicherheitsforschung

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

Hacking Medical Devices

Florian Grunow

In the last few years we have seen an increase of high tech medical devices, including all flavors of communication capabilities. The need of hospitals and patients to transfer data from devices to a central health information system makes the use of a wide range of communication protocols absolutely essential. This results in an increasing complexity of the devices which also increases the attack surface of these devices. We decided to take a look at a few devices that are deployed in many major German hospitals and probably in hospitals around the world. We will focus on the security of these devices and the impact on the patient's safety. The results will be presented in this talk.

Citation: Grunow, F. (2014). Hacking Medical Devices. *Magdeburger Journal zur Sicherheitsforschung*, *1*, 453–455. Retrieved June 22, 2014, from http://www.sicherheitsforschung-magdeburg.de/publikationen.html Version 2014/06/30 19:25

1 Problem Statement

One of our guiding principles at ERNW is »Make the World a Safer Place«. There could not be a topic that matches this principle more than the security or insecurity of medical devices. This is why we started a research project that is looking at how vulnerable those devices are that might be deployed in hospitals around the world. Recently the U.S. Food and Drug Administration (FDA) has published a recommendation concerning the security of medical devices[1] . It recommends that »manufacturers and health care facilities take steps to assure that appropriate safeguards are in place to reduce the risk of failure due to cyber-attack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks«. We thought that we should take a look at how manufacturers deal with security for these devices.

2 Status Quo

If you look at modern medical devices, especially devices that are used for monitoring vital signs, one main feature is networking capability. Hospitals want to monitor multiple patients without a hassle from one central workstation where one nurse is able to see alarms and live data. Many vendors offer the possibility to integrate their devices into the network via LAN, but WiFi is also possible. The protocols used are highly proprietary, which only obfuscates the attack surface. Taking a deeper look we realized that authenticity and integrity of the transported data obviously was not an important requirement. Already known attacks like ARP spoofing and man-in-the-middle attacks work like a charm. Considering that these devices need to have a high availability in case of emergency situations, the impact would be very high. Not to mention the fact that tampering with the data may result in erroneous vital signs being displayed to the doctor.

3 Access to Devices

Getting a hand on these devices is the hardest part. In our experience, vendors are not really responsive when it comes to testing their devices on security. One could buy used medical devices but interesting targets are either not affordable or it's simply not legal to possess or operate them, think of MRIs[2] or X-Ray[3] machines. So we started with devices that every hospital needs and which are not going to threaten your health while gaining a root shell. The technical details in this document might be a little bit unspecific; this is due to the critical nature of the vulnerabilities that we discovered. As we want to make sure that there is no threat to the safety of patients or hospital staff the disclosure process is critical and some of the findings are not patched yet by the vendors. Furthermore the patching process itself might be cumbersome for those devices.

4 Hacking an EEG

The first thing that we looked at was an EEG which is used to measure brain waves. It is split up into two parts, a box that gathers the signals from the patient's brain and a workstation, which displays the data for the doctor. The communication protocol between the workstation and the box is simply UDP with a proprietary data format via the local network. By reversing the protocol we found out that it basically allows extensive control over the box, even during a measurement when the doctor is staring at the workstation screen. There are no checks for integrity or authenticity of the data that passes the network.

5 Hacking Patient Monitors

While this case might not pose a risk on the health of a patient, we found out that similar issues exist in medical devices that will guide a doctor or a nurse in the process of making life critical decisions: Patient monitors. These devices are also capable of communicating over the network and the firmware of many of them can be configured over the network. They might even have wireless capabilities. We found out that the configuration process can be abused to set a configuration on a device that makes no sense at all. It even might be dangerous because it might influence the decision making process of medical personnel.

The ECG measures the electrical activity of the heart[4]. Obviously one of the parameters that are essential to monitor is the heart rate. To set off an alarm when the heart rate of a patient is too low or too high is an essential feature for a patient monitor. These alarm boundaries are to be configured in a reasonable way and the user should not be able to define boundaries that can't even be measured by the device. In the picture above you see the upper alarm boundary of the heart rate alarm set to 30583 and the lower boundary set to -30584. These are values that even a severely sick or perfectly healthy heart would never even get close to. The upper boundary might be somewhere around 220 beats per minute. It is not possible to set these unreasonable limits on the device itself, we had to abuse the configuration process for this to work. This is especially critical when you think of how these devices are used in hospitals. Many patients get connected to a device like this every day, the staff using

[1] http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm r. 2014-03-11

[2] http://en.wikipedia.org/wiki/Magnetic_resonance_imaging r. 2014-03-11

[3] http://en.wikipedia.org/wiki/X-ray r. 2014-03-11

[4] http://en.wikipedia.org/wiki/Electrocardiography r. 2014-03-11

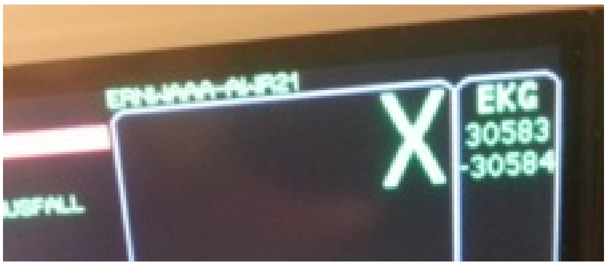

Figure 1: The picture shows alarm boundaries of an ECG

these monitors can be changing multiple times within minutes. Setting unreasonable alarm boundaries on a device might lead to a failure in detecting dangerous heart rates in an emergency situation. In a different case we were able to gain full administrative access to a similar device. We were able to fully remote control the data that was displayed on the device. It was also possible to display fake data on a central monitoring system, which is connected to the devices over the network.

6 Summary

The devices we have seen so far fail to provide an acceptable level of security. No matter how much is spend on safety; if security cannot bet provided all safety considerations are basically gone, too. There will be more to come on this topic as we are in the process of starting cooperations with hospitals to get our hands on devices.

7 About the Author

Florian Grunow is a security analyst at ERNW. He has extensive experience in penetration testing and security assessments of complex technical environments and is specialized on application security. Florian holds a bachelor's degree in medical computer science and a master's degree in software engineering from the university of applied sciences in Mannheim. You can reach him under fgrunow@ernw.de.