Research Article

Radio-Based Cyber-Attacks Against Pacemakers: Assessing Their Chance of Success Under Real Conditions

Mikaëla Ngamboé[1*], José M. Fernandez[1], Katia Dyrda[2]

[1]Department of Computer Engineering and Software Engineering, Information Systems Security Laboratory, Polytechnique Montréal, Montréal, QC, Canada
[2]Department of Medicine, Institut de Cardiologie de Montréal, Université de Montréal, Montréal, QC, Canada

***Corresponding author:** Mikaëla Ngamboé, Department of Computer Engineering and Software Engineering, Polytechnique Montréal, Canada.

Received: 29 September 2021; **Accepted:** 06 October 2021; **Published:** 26 November 2021

Citation: Mikaëla Ngamboé, José M. Fernandez, Katia Dyrda. Radio-Based Cyber-Attacks Against Pacemakers: Assessing Their Chance of Success Under Real Conditions. Cardiology and Cardiovascular Medicine 5 (2021): 591-598.

Abstract

Proofs of concept have shown that certain models of pacemakers are vulnerable to radio-based cyber-attacks. However, to estimate an attack's risk of occurrence, it is not enough to prove its feasibility. It is also necessary to evaluate the attack's chances of success under real conditions. In this study, we evaluate the probability of occurrence of radio-based cyber-attacks against pacemakers. We performed some attacks and documented the difficulties encountered along the way. We then analyzed the effect that these difficulties would have on the outcome of the attacks in real life circumstances. The results of the experiments reveal that the probability of these attacks being conducted in real life is low because of the time and space requirements that are required for their success.

Keywords: Pacemakers, Cardiac Implantable Electronic Devices, CIEDs, Radio-based cyber-attacks, cyber-attacks, Probability of occurrence, Risk.

1. Introduction

Certain models of pacemakers are vulnerable to radio-based cyber-attacks [1-4]. In 2017, the Food and Drug Administration (FDA) warning that nearly half a million pacemakers were vulnerable to unauthorized access allowing a malicious person to reprogram them using commercially available equipment, is a testament to the growing concern about cyber-attacks targeting cardiac implantable devices [5]. Radio-based cyber-attacks consist in intercepting or emitting radio signals for malicious Purposes, they target wireless communications that are not encrypted or those whose authentication mechanism is weak [6, 7].

Regarding the above-mentioned pacemaker models, radio-based cyber-attacks were feasible because the communications between the pacemakers and the external devices they communicate with i.e. the programmer or the home monitor were not encrypted. Specifically, data was transmitted in plain text format via radio waves in the MICS band of service [8]. In such a situation, at least three types of computer attacks are possible. The first one being the interception of the data that the pacemaker transmits when it is interrogated by an external device (eavesdropping attack). The second attack is the jamming of these communications for example, to drain the battery of the pacemaker (Denial Of Services attack). A third potential attack is the transmission of dangerous commands to the pacemaker by impersonating the programmer (command spoofing or command injection attack).

However, to estimate an attack’s risk of occurrence, it is not enough to prove its feasibility. In addition to that, it is necessary to evaluate the attack’s chances of success under real conditions [9]. Until now, no real attack has been performed against a pacemaker, only proofs of concept realized in experimental environments, which are controlled milieus. Nevertheless, the success of the radio-based cyberattacks listed above is conditioned by external factors that are independent of the attackers and not always under their control. The opportunity to attack is an example: in real circumstances the attacker's margin of maneuver is limited in space and time. Indeed, they must be in the place (patient’s house or hospital), at a specific distance from the target (d < 200 m), at a specific time (during an ongoing RF communication) and the number of tries is reduced to the duration of the ongoing communication.
These restrictions make the task arduous for them.

In this study, we evaluate the probability of occurrence of radio-based cyberattacks targeting pacemakers. We do so because until proven otherwise it is the only mean to directly attack a cardiac implantable electronic device. We performed radio-based cyber attacks and documented the difficulties encountered along the way. We then analyzed the effect that these difficulties would have on the outcome of the attacks in real life circumstances, i.e. in a hospital environment or in a patient's home. Based on this analysis, we estimated the probability of occurrence of radio-based cyber attacks targeting pacemakers.

2. Materials and Methods

2.1 Experimental setup

The experimental setup included different tools as demonstrated in Figure 1. The target of the attacks was an Epyra 8 DR-T pacemaker. We used a Biotronik B.O. programmer to establish communication with the cardiac implantable device. The radio-based cyber-attacks were executed using a Software Defined Radio, a transmitter-receiver antenna, and a radio signal processing software. The latter was used to decode the RF signal that the pacemaker transmits and to convert the data we wanted to be transmitted into RF signals.

Software Defined Radio (SDR) are transceiver devices that allow intercepting and broadcasting of RF signals [10]. Model URSP B200 by Ettus Research was used. This SDR can transmit and receive radio waves in the frequency band from 70 MHz to 6 GHz. To do so, a transmitter-receiver antenna is connected to the SDR. We used an SRH-779 antenna, which operates at frequencies up to 435 MHz. Finally, when the SDR receives or must transmit a signal, software is required for processing. There is a wide range of specialized software for RF signal processing. We employed two of them, the Universal Radio Hacker (URH) to record the signals coming from the pacemaker and the Gnu-radio software to transmit signals to the cardiac device.

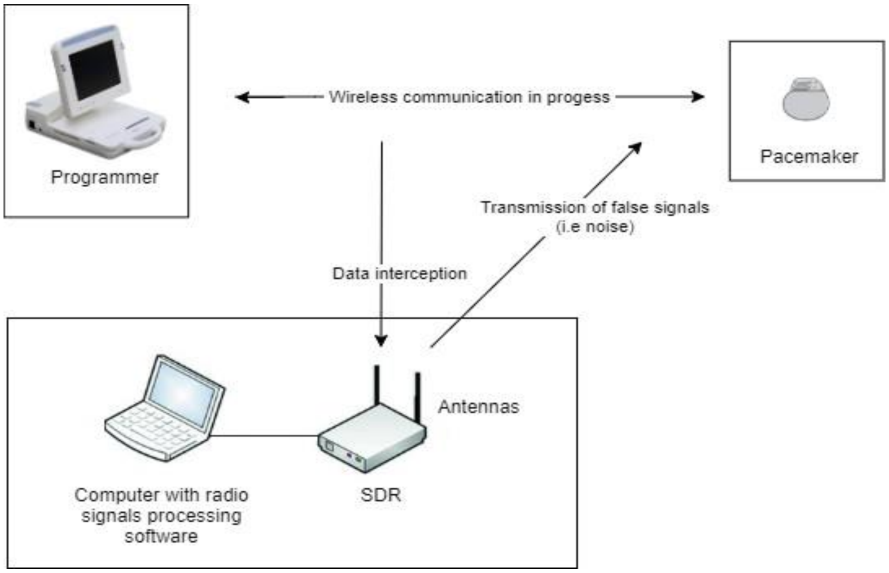

Programmer
Wireless communication in progess
Pacemaker
Transmission of false signals
(i.e noise)
Data interception
Antennas
Computer with radio signals processing software
SDR

Figure 1: experimental setup to perform radio-based attacks against pacemakers

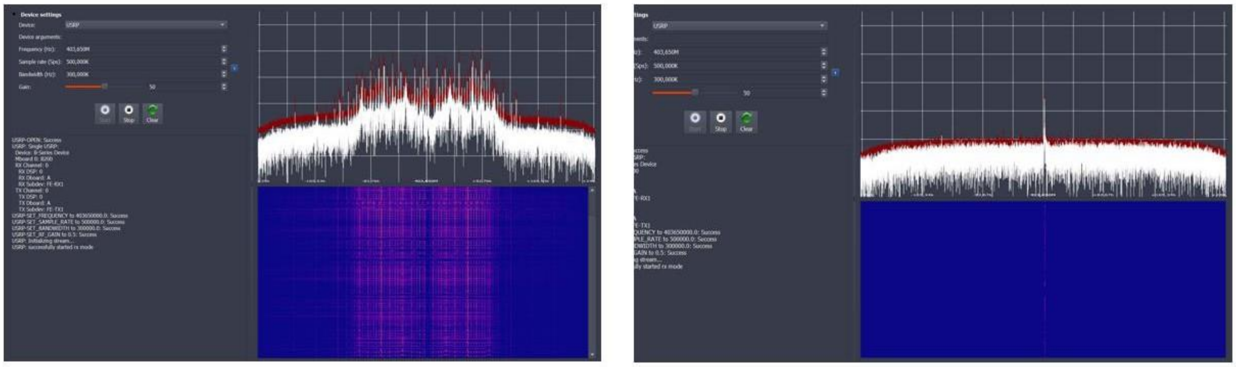
2.2 Execution of the attacks

We performed two different attacks, an eveasdropping attack to intercept the communications between the pacemaker and the programmer and, a Denial of Service (DoS) attack to disrupt these communications.

The goal of the eveasdropping attack is twofold: to obtain sensitive patient data and the operation commands of the programmer. The last technique is called reverse engineering and it allows to master the way a device or a computer system operates. Reverse engineering is a legitimate way of learning; however, some attackers abuse it. Indeed, if the goal of attackers were to inject dangerous commands to the pacemaker, they would first obtain the operating commands of the programmer and then, manipulate them for malicious purposes.

When executing the eveasdropping attack, the SDR was configured in reception mode and the antenna was tuned to the target's reception frequency. The wireless communication was initiated by Interrogating the pacemaker with the programmer's magnetic head. Once the communication was initiated, the SDR received the data which was recorded by computer by means of the URH software.

A DoS attack aims to disrupt or make unavailable a service, in our case we wanted to interrupt the communication in progress between the pacemaker and the programmer. Indeed, once the communication was initiated, we transmitted noise in the frequency at which the pacemaker was receiving. For the attack to be successful, the power of the noise signal must be greater than that of the signals transmitted by the target.



Device settings
Device: USRP
Device arguments:
Frequency (Hz): 403,650M
Sample rate (Sps): 500,000K
Bandwidth (Hz): 300,000K
Gain: 50

```
USRP-OPEN: Success
USRP: Single USRP:
  Device: B-Series Device
  Mboard 0: B200
  RX Channel: 0
    RX DSP: 0
    RX Dboard: A
    RX Subdev: FE-RX1
  TX Channel: 0
    TX DSP: 0
    TX Dboard: A
    TX Subdev: FE-TX1
USRP-SET_FREQUENCY to 403650000.0: Success
USRP-SET_SAMPLE_RATE to 500000.0: Success
USRP-SET_BANDWIDTH to 300000.0: Success
USRP-SET_RF_GAIN to 0.5: Success
USRP: Initializing stream...
USRP: successfully started rx mode
```

ttings
USRP
ments:
z): 403,650M
(Sps): 500,000K
z): 300,000K
50

```
ccess
SRP:
es Device
00
A
E-RX1
A
E-TX1
QUENCY to 403650000.0: Success
PLE_RATE to 500000.0: Success
DWIDTH to 300000.0: Success
GAIN to 0.5: Success
g stream...
lly started rx mode
```

Figure 2: Eavesdropping attacks to intercept the ongoing communication between the pacemaker and the programmer. The first picture shows the RF signal which corresponds to the programmer's interrogation command. The second one shows the answer of the pacemaker [12].

2.3 Estimation of the probability of occurrence of the attacks

An attack's probability of occurrence represents the chance that the threat materializes with success. By success we mean the achievement of the attack's goal. Regarding the four types of radio-based attack we mentioned in the introduction, the attack objectives are: the interception of data (eavesdropping attack), the disruption of wireless communications (DoS attack), the emission of dangerous commands (command spoofing or command injection attack) and the transmission of false data (data falsification attack).

When deciding if carrying out an attack, attackers evaluate three key aspect, their capability (c), opportunity (o) and motivation (m) for attack. Capability represents the technical complexity of the attack and the technical and material resources available to the attacker to carry out the threat. Opportunity is the chances of the latter having access to the target and being there at the right moment. Motivation reflects the attacker's degree of interest in accomplishing the threat.

We calculate the probability of occurrence for each type of attack as the sum of the three characteristics capacity (c), opportunity (o) and motivation (m). The c,o,m values vary from1 to 4, with 4 corresponding to a higher value.

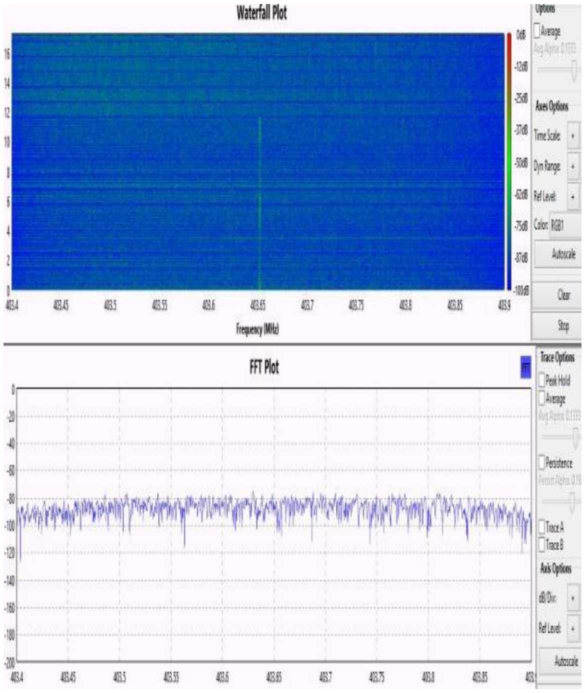


Figure 3: Interception of the pacemaker signal with the antenna and the SDR located at 0.3 meters [12].

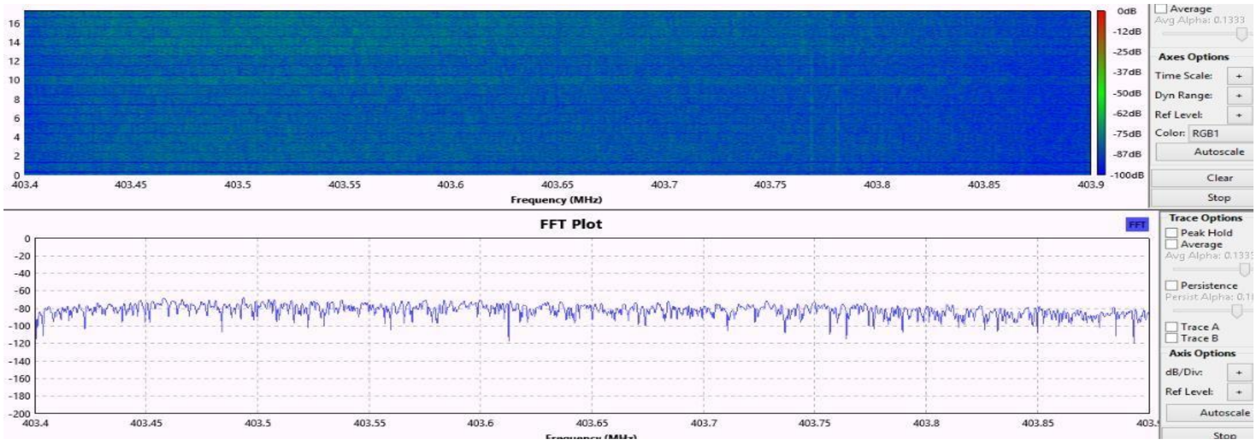


Figure 4: Interception of the pacemaker signal with the antenna and the SDR located at 0.5 meters [12].

3. Results

The results of the experiments reveal that the probability of occurrence of radio-based cyber attacks against pacemakers is low in comparison with other types of computers attacks. In terms of capability, the attacks are simple to perform. Indeed, there is an abundance of information available, the equipment required is low cost and the software needed is user friendly. However, the opportunity to execute these attacks in real life is low because of the time and space requirements that their success requires. Specifically, the attacker must be near to the target while a wireless communication is in progress and must do so without being noticed. As we will discuss later, these requirements are difficult to meet.

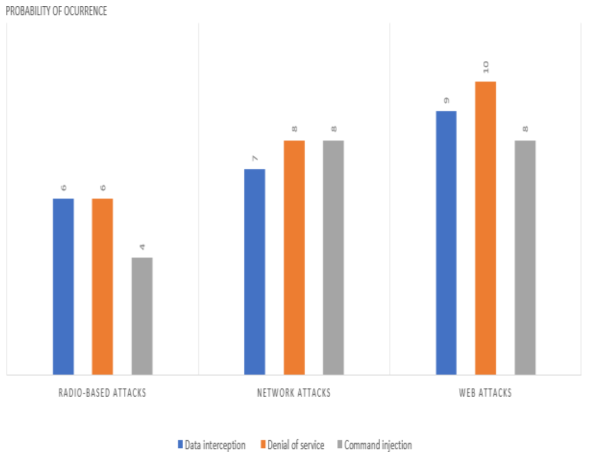


Figure 5: Probability of occurrence of computer attacks against pacemakers. The lower legend represents three attack goals, the abscissa axis shows the probability of achieving them by means of radio-based attacks, network attacks and web attacks.

Discussion

We noticed that several conditions must be simultaneously satisfied to exploit the wireless communications between the pacemaker and the programmer. First, the adversary must be close to the target at the time of the attack. As illustrated in Figures 2 and 3, the distance between the SDR's antenna and the pacemaker had to be strictly less than half a meter. Otherwise, we were not able to see the signals that the device was transmitting. Second, the SDR's antenna must be exactly tuned to the working frequency of the pacemaker or the programmer. This premise is problematic in the sense that both devices randomly change their frequency at each session. Before performing the attack, we had to scan the MICS frequencies with a spectrum analyzer to determine the frequency on which our targets were transmitting and receiving. This could take a few minutes if one of the devices was using a frequency at the end of the MICS channel. Therefore, for an attack to succeed on the first try, the adversary must have 10 SDRs, each tuned to one of the carrier frequencies of the MICS channel. Finally, the last condition concerns the ambient noise, it must be low, the signals that the pacemakers transmit have a low power, a high ambient noise makes them unnoticeable. Therefore, all these conditions reduce not only the opportunity to attack a pacemaker but also the motivation to do so, since the attackers expose themselves to being noticed. They could accomplish the same attack objectives by other means [9,11,12].

In this line of thought, the results of a recent study [9] reveal that the telemetry and IP connectivity features of the external devices with which pacemakers interact constitute a potential attack vector. Moreover, the outcomes of the research indicate that the probability of occurrence of attacks that exploit the above-mentioned features is higher than that of radio-based attacks. It is worth noting that the term telemetry refers to remotely accessing a computer system, as an example, the programmer's update is done by telemetry. More specifically, by accessing the device through the network.

Furthermore, an IP connectivity functionality refers to a computer system's capability to access or be accessed by internet, such is the case of home monitor. These devices collect data from the pacemaker and then transmit the information over the Internet to a cloud database so that practitioners can consult the information that is stored in the database through a web application. As depicted in figure 4, it is possible to reach the same attack objectives as those of the radio-based attacks by carrying out network attacks or web attacks against the external devices. On the one hand, the opportunity to attack is higher since networks (private or public as internet) are always accessible. On the other hand, the motivation of the attackers is higher because they are less likely to be caught as there is no need to be on site when performing the attack. Thus, although the risk of directly attacking a pacemaker is a threat, it is low and therefore acceptable. However, it is a priority to strengthen the security of the external systems on which pacemakers depend, the networks in which these systems are deployed, and the cloud-based medical services that depend on these external systems.

Conclusion

Although the risk of directly cyberattacking a pacemaker is a threat, this risk is low and therefore acceptable. The real, and greater risk lies in computer networks, and there are several solutions to mitigate this risk. It is thus within the reach of health care providers and patients to protect themselves against such computer attacks by using only secure computer networks to transmit data and access devices.

Acknowledgement: None

Financial Disclosure: None to declare.

Conflict of Interest: None

References

1. Marin E, Singelée D, Garcia FD, Chothia T, Willems R & Preneel B. On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In Proceedings of the 32nd annual conference on computer security applications (2016): 226-236.
2. Rios B & Butts J. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. WhiteScope, sl (2017).
3. Halperin D, Heydt-Benjamin T S, Ransford, B, Clark S S, Defend B, Morgan W ... & Maisel WH. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero- power defenses. In 2008 IEEE Symposium on Security and Privacy (2008) : 129-142.
4. ICS-CERT. Advisory icsma-17-241-01. Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities (2017).
5. US Food & Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication (2017).
6. Heinäaro K. Cyber attacking tactical radio networks. In 2015 International Conference on Military Communications and Information Systems (ICMCIS) (2015): 1-6.
7. Salahdine F & Kaabouch N. Security threats, detection, and countermeasures for physical layer in cognitive radio networks:

A survey. Physical Communication 39 (2020): 101001.

8. Savci H S, Sula A, Wang Z, Dogan NS & Arvas E. MICS transceivers: regulatory standards and applications [medical implant communications service]. In Proceedings. IEEE SoutheastCon (2005): 179-182.
9. Ngamboé M, Berthier P, Ammari N, Dyrda K & Fernandez JM. Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED). International Journal of Information Security (2020): 1-25.
10. Hung PD & Vinh BT. Vulnerabilities in IoT devices with software-defined radio. In 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS) (2019): 664-668.
11. Williams PA & Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices (Auckland, NZ), 8 (2015): 305.
12. Ngamboe Mvogo, M. S. (2019). Analyse du risque en matière de cybersécurité de l'écosystème des dispositifs électroniques cardiaques implantables (DECI) (Masters thesis, Polytechnique Montréal). Retrieved from https://publications.polymtl.ca/3877/.