Security and privacy issues of data-over-sound technologies used in IoT healthcare devices

Carlos Cilleruelo  
Computer Science Department  
Universidad de Alcalá  
Alcalá de Henares, Spain  
carlos.cilleruelo@uah.es

Javier Junquera-Sánchez  
Computer Science Department  
Universidad de Alcalá  
Alcalá de Henares, Spain  
javier.junquera@uah.es

Luis de-Marcos  
Computer Science Department  
Universidad de Alcalá  
Alcalá de Henares, Spain  
luis.demarcos@uah.es

Nicolas Logghe  
Computer Science Department  
Universidad de Alcalá  
Alcalá de Henares, Spain  
nicolas.logghe@edu.uah.es

Jose-Javier Martinez-Herraiz  
Computer Science Department  
Universidad de Alcalá  
Alcalá de Henares, Spain  
josej.martinez@uah.es

Abstract—Internet of things (IoT) healthcare devices, like other IoT devices, typically use proprietary protocol communications. Usually, these proprietary protocols are not audited and may present security flaws. Further, new proprietary protocols are designed in the field of IoT devices, like data-over-sound communications. Data-over-sound is a new method of communication based on audio with increasing popularity due to its low hardware requirements. Only a speaker and a microphone are needed instead of the specific antennas required by Bluetooth or Wi-Fi protocols. In this paper, we analyze, audit and reverse engineer a modern IoT healthcare device used for performing electrocardiograms (ECG). The audited device is currently used in multiple hospitals and allows remote health monitoring of a patient with heart disease. For this auditing, we follow a black-box reverse-engineering approach and used STRIDE threat analysis methodology to assess all possible attacks. Following this methodology, we successfully reverse the proprietary data-over-sound protocol used by the IoT healthcare device and subsequently identified several vulnerabilities associated with the device. These vulnerabilities were analyzed through several experiments to classify and test them. We were able to successfully manipulate ECG results and fake heart illnesses. Furthermore, all attacks identified did not need any patient interaction, being this a transparent process which is difficult to detect. Finally, we suggest several short-term solutions, centred in the device isolation, as well as long-term solutions, centred in involved encryption capabilities.

Index Terms—Communication system security, Data security, Internet of Things, Health devices

I. INTRODUCTION

Nowadays multiple IoT healthcare devices are being used by hospital staff and patients. Over the years, Implantable Medical Devices (IMDs) and Implantable Cardiac Defibrillators (ICDs) have been adding wireless communication capabilities. But other IoT healthcare device has also been improving their interconnectivity and wireless communications technologies, like insulin pumps or mobile electrocardiographs. The patients can carry these small electrocardiographs where they can perform periodic electrocardiograms (ECGs) that will be sent to their corresponding medical specialist. These novel IoT devices facilitate monitoring and earlier diagnosis of patients, avoiding numerous hospital visits. Similar to other devices in the IoT industry, some of these devices are using proprietary protocols or involve new methods of communications. One of these new emerging communications technologies used for healthcare devices is known as data-over-sound.

Data-over-sound presents an alternative to traditional radio frequency (RF) communications granting several advantages over RF. Data-over-sound avoids the necessity of using specific hardware since just a microphone and speaker are needed to establish the communications. This also has the advantage of bypassing other problems like radio frequency interference. As mentioned these advantages bring several benefits, but the cybersecurity of novel protocols and implementations need to be evaluated. Data-over-sound protocols are a low-cost solution in comparison with Wi-Fi or Bluetooth protocols, but due to its novelty, this technology has been less audited and tested in applications, like IoT healthcare devices where sensitive data is being transmitted. It is also necessary to take into account, that even though attacks against external IoT devices like mobile electrocardiographs do not represent the same risk as IMDs or ICDs devices, they still manage healthcare information which is taken into account for medical decisions.

This paper presents an analysis of an IoT healthcare device, a mobile electrocardiograph, which is capable of maintaining data-over-sound communication with a smartphone. We performed reverse engineering analysis of this IoT healthcare device and its data-over-sound protocol, following a black-box approach. This process allowed us to analyze the data-over-sound proprietary protocol used in this IoT healthcare device and discover several cybersecurity vulnerabilities.

In summary, we make the following contributions:

- We reverse engineer and analyse an IoT healthcare device capable of performing wireless data-over-sound commu-
• We identified several cybersecurity vulnerabilities in this specific device due to the nature of the data-over-sound protocol used and its implementation.
• We present short-term and long-term solutions in order to address and mitigate the discovered vulnerabilities.

Besides these contributions, all vulnerabilities and problems presented in this paper followed a responsible disclosure process. The manufacturer and the Cybersecurity and Infrastructure Security Agency (CISA) were notified, prior to publication and submission of this paper. And as an additional step, all references to the specific product and manufacturer have been omitted from this paper, since the manufacturer is still working on possible mitigation solutions.

The remainder of this paper is structured as follows. Section II presents an overview of the related work, a general view of the security status in healthcare devices, and information about data-over-sound technology protocols used in the industry and their evolution. Section III describes the methodology for the analysis of the device and the laboratory setup used for experimentation. Section IV shows the processes taken for reverse-engineering the data-over-sound protocol and presents the weaknesses found. Section V presents the different cybersecurity vulnerabilities and attacks discovered. Section VI analyzes the attacks and proposes short-term and long-term solutions. Finally, Section VII provides concluding remarks.

II. RELATED WORK

Cybersecurity problems in healthcare devices are not something new. Several papers and researches have explored the lack of cybersecurity measures in technological healthcare devices [1]. Usually, these researches have been focused on Implantable Medical Devices (IMDs), like pacemakers [2] or Implantable Cardiac Defibrillators (ICDs) [3]. The evolution of medical devices into connected devices or healthcare IoT has provoked the discoveries of numerous vulnerabilities [4]. The use of Radio Frequency Identification (RFID), Wi-Fi or other proprietary radio protocols [3] are normally part in IoT healthcare devices without implementing proper cybersecurity measures.

Many possible solutions to these attacks have been presented in recent years. Several propositions involve the use of external devices acting like proxies [5] [6] to protect the communications on healthcare devices. Although the use of proxies mitigates some attacks, it has been demonstrated incapable of offering a full security solution, being affected by Man-In-The-Middle (MITM) attacks [7] or eavesdropping using MIMO-based attacks [8]. On the other hand, other research papers involve the use of cryptography algorithms to protect healthcare device communications [9]. However, the use of cryptography usually implies the need for more computational power on devices or dedicated hardware. This directly affects the manufacturing cost and energy consumption of IoT devices.

Nevertheless, even though there are numerous researches around different healthcare devices and how to implement cybersecurity measures on these devices, the lack of actual regulations and standards around IoT security or medical device security results in the discovery of serious vulnerabilities. There are some U.S regulations like Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, centred in healthcare data regulation but they usually do not present any clear indications on how to protect private information or cybersecurity measures to be taken into account. This establishes the necessity of new cybersecurity industry standards like the proposed by Strielkina et al. [10]. These standards should be included in mandatory healthcare regulations, independent of novel technological solutions, forcing new IoT healthcare devices to be cybersecurity compliant.

A. Data-over-sound communications

As previously mentioned the device studied in this article uses data-over-sound communications. Due to the usage of this novel type of communication, it is necessary to review and explain the status of data-over-sound communications, also known as Audio Data Transmission (ADT). Data-over-sound presents an alternative to traditional radio frequency communications and has been successfully used in several scenarios. Zhang et al. successfully develop an emergency warning system using digital audio broadcast [11]. And independently of research projects, several companies are developing data-over-sound communication protocols [12]. Additionally to the previously mentioned works, several open source projects that implement data-over-sound libraries can be found on GitHub [13] [14].

III. METHODOLOGY

A. Thread modeling - STRIDE

Before performing any test over the IoT healthcare device, we built a threat model based on STRIDE framework [15]. This framework provides a mnemonic for security threats, classified in six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of privilege. These threats face Authentication, Integrity, Non-repudiation, Confidentiality, Availability and Authorization; respectively. STRIDE is used because it also offers a systematic manner to develop the analysis. Even though our research is focused on data-over-sound communications, obtaining the complete landscape of the system allowed us to detect and assess the impact of a vulnerability in the ECG recording process. Figure 1 shows a Data Flow Diagram (DFD, also known as Threat Modelling Diagrams [16]), of an IoT healthcare device and its communications. This DFD allows us to obtain a software-centric vision of the architecture from where we can characterize the threats.

The DFD, along with the STRIDE categorization, allows both narrowing the attack surface exposed to each threat, as well as measuring the risk it contributes to the entire system. Thus, we can deduce the scope affected by a threat acting over the HR Audio flow.
B. Laboratory setup

Figure 2 shows our laboratory setup, composed of a laptop, the IoT healthcare device and the external microphone. More sophisticated equipment like a directional microphone could also be used to extend the range of possible attacks. But taking into account, that all the device communications are performed via sound, any device with a microphone and speakers could be used as a transceiver. As support tools, several software audio solutions have been used in the analysis and experiments, like Audacity [17] and Sonic Visualiser [18]. Audacity allowed us to capture and modify data-over-sound communications, and Sonic Visualizer allows us to perform different visualisations of these communications. Also, it is necessary to mention that all the analyses have followed a black-box reverse-engineering approach.

IV. REVERSE-ENGINEERING DATA-OVER-SOUND COMMUNICATIONS

First of all, we studied the possibilities of communication of the IoT device. After analyzing the mobile application, we realized that the IoT healthcare device was sending information through audio. The mobile application requested microphone permissions and asks for the deactivation of mobile NFC communications. However, we were unable to listen to anything so we decided to make some recordings using a microphone. Initially, the recording suggested that the transmission was being done in a very low volume: the manufacturer instructions state that the device must be near the phone, and there was just a faint waves in the wave plot generated by Audacity.

Later on we proceeded to take other recordings, using Audacity, while the IoT healthcare device was producing an ECG. After analyzing the audio recordings with a spectrogram (see Figure 3)), we realized there was data in the high frequency band of the spectrum. Hence, we are facing some kind of data-over-sound protocol. This analysis also showed that the IoT device uses ultrasounds to perform the transmission and communications. Subsequently, we performed a waterfall analysis, that showed us that the frequency oscillates over time around 19.200kHz. This suggests that the data values could be modulated using FM.

A. Data-over-sound characterization

Anything over 10kHz is pretty much inaudible and also used in many other applications since most everyday sounds (included other sound-based control systems, like phone signalling [19]) occur at frequencies below 4kHz. This situation, makes higher frequencies a perfect medium for transmitting
Fig. 3. Spectrogram of the IoT device audio

data. Sounds somewhat below 20 kHz, which are also inaudible to a human listener, are still considered to be in the ultrasonic range and can be captured by common microphones. This provides a limited frequency band that can be used for data transmission.

Subsequently, we performed a waterfall analysis, showing that the frequency oscillates over time around 19.200 kHz. Due to the oscillation range, the chart also suggests the data values could be modulated over frequency (i.e., Frequency Modulation, or FM). In FM, the values are modulated in the wave increasing or decreasing its frequency (for encoding up and low values, respectively).

To evaluate how the ECG signal was transmitted, we developed a fuzzing script. The experiment proceeded as follows:

1) Create the message to transmit: As the ECG mobile application draws the ECG in live-time, our script generates a sinus function as a baseband signal, to check how it interferes with the cardiogram drawing. To emulate a heartbeat of 60bpm, we discretized the sinus, obtaining 44100 values of one period (i.e., a 44100 values audio sampling). It transforms the sinus formula into an array with values between $-1$ and $1$.

2) Modulate the message in FM: Here, we also used a sinusoidal carrier to generate a reproducible WAV file. We calculated the discrete values that the signal should have, using the sinus formula. Using the values of the message, we applied them to vary the frequency of the signal. As the WAV file is also discrete (i.e., also has a sampling rate, set in 44100 samples per second), we applied the formulas from the Equation 1 to obtain each sample $i$. Where $t$ is the time of the period where the sample has to be calculated; $f_i$ is the frequency of the signal in base to the message value $m_i$, and $\text{sample}_i$ is the value of the signal for the sample $i$.

\begin{align}
\nonumber t &= (i \mod 44100)/44100 \\
\nonumber f_i &= 19200 + 1000 \times m_i \\
\nonumber \text{sample}_i &= \sin(2 \times \pi \times f_i \times t)
\end{align}

3) Observe the results in the mobile application

After analyzing for the first time the figure drawn in the application, following the playing of the WAV file, the image resulted in the representation of a sinus wave. This information allowed us to conclude that the IoT device did not perform any additional encoding to the ECG signal but modulated it in frequency.

V. RESULTS

The previously reverse engineering analysis of the communication protocols of the device allows us to discover several cybersecurity vulnerabilities. These vulnerabilities resulted in several types of active and passive attacks which are presented following the STRIDE methodology.

A. Spoofing

Our analysis of the proprietary data-over-sound protocol demonstrated the lack of encryption and authentication in the communication process between the IoT device and a smartphone. This lack of encryption in the communication directly leads to the possibility of performing spoofing attacks.

This makes possible the generation of fake signals and altering ECG values based on the objectives of an attacker. For example, as shown in Figure 4 it is possible to generate a signal that will generate a fake ECG, as shown in Figure 4. Using this same technique is also possible to generate ECG classified as tachycardia and other heart issues.
Fig. 4. Fake ECG generated through custom data-over-sound

B. Tampering

This lack of encryption and authentication could also turn into a more sophisticated scenario like tampering. Whenever a patient is using the device, an evil twin attack can be done. In the event that the user is going to take a measurement, it is possible to simultaneously generate a stronger signal, that will affect the results of the ECG.

We were able to impersonate the genuine device and tamper an active ECG session from a distance of 25m just using a laptop. An attacker with a directional speaker, or with a louder one, could be able to perform this attack from a larger distance.

C. Repudiation

The easiest of these attacks can be a replay attack, where an attacker is able to capture a wireless communication and later replay it against the device. Our results show that there is no mechanism to prevent replay attacks; any previously captured data can be sent multiple times. The device lacks any type of repudiation technology, any data-over-sound captured can be replayed at any time and its transmission will always be accepted.

D. Information disclosure

Following the lack of encryption and authentication, an attacker can be centred on stealing private information. The messages exchanged between the devices did not seem to include patient data, like names or usernames, but it is possible to recover the ECG data sent from other devices. Passive adversaries can compromise the patient’s privacy just by eavesdropping on the wireless sound channel while there is ongoing communication. On the other hand, this attack is limited due to the fact that the attacker has to be near the target patient. But it is also needed to take into account that adversaries could use sophisticated equipment, like a directional microphone to extend the distance from which they can perform these attacks. However, being this a passive attack, the attacker would need to wait until the device exchanges data to complete a successful eavesdropping attack.

E. Denial-of-Service

The lack of security measurements in the data data-over-sound protocol used in the IoT healthcare device also results in Denial-of-Service (DoS) vulnerabilities. An attacker can easily perform a DoS attack by continuously sending noise in frequencies near 20kHz. Therefore, jamming the genuine sound generated by the IoT healthcare device is possible by playing alternative sounds at a higher volume, as will still be inaudible by humans.

VI. Discussion

First of all it necessary to take into account that the severity of these attacks are limited due to the necessity of being in a relatively short distance between the attacker and the objective, around 25 meters. After taking this into account, the device lacks of any minimal security measures and the severity of this attacks could be classified as medium just because of the previously mentioned context. Furthermore, all the presented attacks were further tested to determine how easy it could be to tamper the signal without any special hardware devices (e.g., just with a computer, or a smartphone).

A. Short-term solutions

Short-term measures that can be applied to resolve the mentioned issues could be the use of the IoT healthcare device in an isolated and close environment. If we do not have anyone near our ECG measurement and we are in a close environment, we make it practically impossible to be able to perform the previously mentioned attacks. This is a possible short-term and easy solution. Another recommendation is to bring the device as close as possible to the smartphone. If the IoT device is closer to the microphone smartphone than the attacker, it will make more difficult some attacks, like replay or tampering. Because the strength of our data-over-sound signal will be greater than the attacker.

B. Long-term solutions

The use of properly authenticated and encrypted channels can be a possible countermeasure to the proposed attacks. The usage of data-over-sound communications does not imply that encryption and authentication can not be applied. For example, previously mentioned commercial solutions like Sonarax [12] uses encryption for its implementation. The problem of the analysed IoT device is not the usage of data-over-sound communications but its implementation.

Even though a device can only transmit data (i.e., it has no input capabilities), it could have some type of identification. This identification could allow the user to pre-register the IoT device before establishing communications. This identification could be encoded as a QR code signed by the manufacturer,
or use any type of signed beacon [20]. Moreover, this spoofing mitigation will also prevent possible replay attacks [21]. But with a pre-registered device, the transmissions could be authenticated using any type of TAN code, as proposed by Starnberger et al. [22]. This protection could also allow the mitigation of tampering attacks.

On the other hand, denial of service attacks present a difficult challenge. Even though there exist some approaches against jamming in other transmission channels (like channel-hopping in RF [23]), the data-over-sound technologies are not very reliable in that aspect [24].

VII. CONCLUSION

In this work we analyzed the security and privacy of an IoT healthcare device capable of perform data-over-sound communications. To accomplish this objective we acquired a novel and small IoT device capable of perform ECGs. This device was analyzed following the STRIDE thread modeling methodology, and as a result several vulnerabilities were identified. All the presented work has been notified to CISA and the device manufacturer, following a responsible disclosure process. But the manufacturer is still working on mitigation solutions, so we avoid mentioning the manufacturer and device name in this paper. Moreover it is necessary to mention that all the previous processes explained in this article have been created following a black-box approach.

This work also discovered several cybersecurity vulnerabilities. These attacks are only limited due to the communication range allowed by the device since the attacker needs to stay at a distance shorter than 25 meters. Base on our experience the most critical attacks are the ones based on tampering and spoofing of communications. An attacker could generate a fake ECG with a tachycardia or other heart anomaly, like atrial fibrillation, which could make the patient think that he is having a health issue.

Finally, we proposed some possible solutions to these problems. Short-term solutions are based on the location and isolation of the device. Isolation solutions are not a viable long-term solution. These are difficult to apply on IoT devices because they require hardware changes. We suggest to implement properly encrypted data-over-sound communications as a long-term solution.

VIII. FUNDING & ACKNOWLEDGEMENTS

This project has received funding from the European Union’s Horizon 2020 Research and innovation programme under grant agreement No. 826284.

REFERENCES

[1] M. Khera, “Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications,” Journal of Diabetes Science and Technology, vol. 11, no. 2, pp. 207–212, Mar. 2017, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/1932296816677576

[2] J. L. Beavers, M. Faulks, and J. Marchang, “Hacking NHS Pacemakers: A Feasibility Study,” in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGSS), Jan. 2019, pp. 206–212.

[3] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, “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, ser. ACSAC ’16. Association for Computing Machinery, pp. 226–236. [Online]. Available: https://doi.org/10.1145/2991075.2991094

[4] “Medtronic Conexus Radio Frequency Telemetry Protocol (Update C).” [Online]. Available: https://us-cert.cisa.gov/indicators/ICSMA-19-080-01

[5] “They can hear your heartbeats | Proceedings of the ACM SIGCOMM 2011 conference.” [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2018436.2018438

[6] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, “IMDGuard: Secure implantable medical devices with the external wearable guardian,” in 2011 Proceedings IEEE INFOCOM, Apr. 2011, pp. 1862–1870. ISBN: 0743-166X.

[7] M. Rostami, W. Burleson, F. Koushanfar, and A. Juels, “Balancing security and utility in medical devices?” in Proceedings of the 50th Annual Design Automation Conference, ser. DAC ’13. New York, NY, USA: Association for Computing Machinery, May 2013, pp. 1–6. [Online]. Available: https://doi.org/10.1145/2463209.2488750

[8] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, “On Limitations of Friendly Jamming for Confidentiality,” in 2013 IEEE Symposium on Security and Privacy, May 2013, pp. 160–173, issn: 1081-0681.

[9] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, “Proximity-based access control for implantable medical devices,” in Proceedings of the 16th ACM conference on Computer and communications security, ser. CCS ’09. New York, NY, USA: Association for Computing Machinery, Nov. 2009, pp. 410–419. [Online]. Available: https://doi.org/10.1145/1653662.1653712

[10] A. Strelkina, O. Illiashenko, M. Zhydenko, and D. Uzun, “Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment,” in 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), May 2018, pp. 67–73.

[11] H. Zhang, G. Wang, M. Lu, D. Wang, and P. Xu, “Emergency Warning and Bidirectional Communication via Digital Audio Broadcast,” IEEE Transactions on Consumer Electronics, vol. 65, no. 2, pp. 150–159, May 2019, conference Name: IEEE Transactions on Consumer Electronics.

[12] “Sonarax | Contact Tracing & Secure Touch-less Technology.” [Online]. Available: https://www.sonarax.com/

[13] R. Rypula, “robertryppula/AudioNetwork,” Apr. 2021, original-date: 2016-04-18T19:42:21Z. [Online]. Available: https://github.com/robertryppula/AudioNetwork

[14] “quiet/quiet,” Jun. 2021, original-date: 2016-01-15T00:00:28Z. [Online]. Available: https://github.com/quiet/quiet

[15] kexugit, “Uncover Security Design Flaws Using The STRIDE Approach.” [Online]. Available: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[16] A. Shostack, Threat Modeling: Designing for Security, 1st ed. Wiley.

[17] “Audacity.” [Online]. Available: https://www.audacityteam.org

[18] “Sonic Visualiser.” [Online]. Available: https://www.sonicvisualiser.org/

[19] R. Sharma, K. Kumar, and S. Vig, “DTMF Based Remote Control System,” in 2006 IEEE International Conference on Industrial Technology, Dec. 2006, pp. 2380–2383.

[20] R. Couto, J. Leal, P. M. Costa, and T. Galvão, “Exploring ticketing approaches using mobile technologies: QR codes, NFC and BLE,” in 2015 IEEE 18th International Conference on Intelligent Transportation Systems, pp. 7–12. ISSN: 2153-0017.

[21] P.-Y. Lin, “Distributed secret sharing approaches using cheater prevention based on QR code,” vol. 12, no. 1, pp. 384–392, conference Name: IEEE Transactions on Industrial Informatics.

[22] G. Starnberger, L. Frohofer, and K. M. Goeschka, “QR-TAN: Secure mobile transaction authentication,” in 2009 International Conference on Availability, Reliability and Security, pp. 578–583.

[23] C.-M. Lee, J.-S. Lin, Y.-P. Hsu, and K.-T. Feng, “Design and Analysis of Optimal Channel-Hopping Sequence for Cognitive Radio Networks,” in 2010 IEEE Wireless Communication and Networking Conference, Apr. 2010, pp. 1–6, ISSN: 1588-2901.

[24] The challenges of developing data over sound technology. [Online]. Available: https://www.sonarax.com/post/why-its-so-challenging-to-develop-data-over-sound-technology-why-the-other-protocols-failed