Spring 2023

A Study of Issues and Mitigations on DDoS and Medical IoT Devices

Jing-Chiou Liou
Kean University, jliou@kean.edu

Robin Singh
Kean University, singhro@kean.edu

A Study of Issues and Mitigations on Ddos and Medical Iot Devices

Robin Singh and Jing-Chiou Liou

***Abstract---* The Internet of Things (IoT) devices are being used heavily as part of our everyday routines. Through improved communication and automated procedures, its popularity has assisted users in raising the quality of work. These devices are used in healthcare in order to better collect the patient's data for their treatment. They are generally considered safe and secure. However, there is some possibility that some loopholes do exist which manufacturers do need to identify before some hacker takes advantage of them. For this study, we focused on two medical IoT devices which are pacemakers and hearing aids. The aim of this paper is to identify if there is any likelihood of these medical devices being hijacked and used as a botnet in Distributed Denial-Of Service attacks. Moreover, some mitigation strategies are being proposed to better secure these devices and make them less vulnerable to hijack.**

Keywords—*DDoS, hearing aid, pacemaker, security risk.*

I. INTRODUCTION

The Internet of Things (IoT) devices are low resourced and low powered devices that are connected to the internet via Wi-Fi or Bluetooth. These devices can be remotely configured and controlled via software applications or backend servers [6]. Some popular examples of medical IoT devices are hearing aids, pacemakers, infusion pumps, insulin pumps etc.

Since IoT devices are low powered and low processing devices, the security implementation to them is quite limited. In the past, there have been cases when IoT devices have been hacked that demonstrate their lack of security. For example, in 2016, popular malware Mirai was hijacking a number of IoT devices and turning them into botnets so that they can take commands from the C & C server of the attacker [7]. IHS Market said the number of connected devices will be 75.4 billion in 2025 [6].

The main cause for concern for hacked IoT devices is in performing Denial-Of-Service (DoS) attacks. DoS and DDoS (Distributed-Denial-Of-Service) attacks are some of the most common and dangerous attacks on modern networks that could really hinder a business's workflow. A DoS attack is an attempt to compromise availability by hindering or blocking completely the provision of some service. This attack is based on the fact that any device has operational limits by overloading a system with so much traffic that will take the system offline temporarily. DDoS attacks using IoT devices are cyber-attacks that cause bandwidth overload by increasing traffic on the network to make services unavailable [8].

In this study, we will be reviewing the security of various medical IoT devices and how these devices could be compromised to perform an amplification-based DDoS attack. We further proposed some possible methods of effectively mitigating the risk of these IoT medical devices turning into botnets. The devices we reviewed in this study are hearing aid and pacemaker.

II. IoT NETWORK ARCHITECTURE

IoT devices are different from traditional network devices, in the sense that they perform different functions and have the ability to operate in dynamic surroundings. These smart IoT devices are equipped with sensors connected to the internet that are uniquely identifiable, communicating with each other to perform complex tasks. As such, these devices require the ability to collect, process, and transmit data through various channels [5].

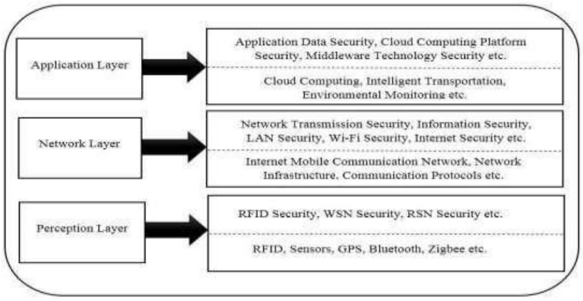
Application Layer
Application Data Security, Cloud Computing Platform Security, Middleware Technology Security etc.
Cloud Computing, Intelligent Transportation, Environmental Monitoring etc.
Network Layer
Network Transmission Security, Information Security, LAN Security, Wi-Fi Security, Internet Security etc.
Internet Mobile Communication Network, Network Infrastructure, Communication Protocols etc.
Perception Layer
RFID Security, WSN Security, RSN Security etc.
RFID, Sensors, GPS, Bluetooth, Zigbee etc.

Fig. 1 Three layered IoT architecture [18]

IoT Networks consist generally of a three-layer architecture [5], [18]. Layers consisting of the Application layer, Network layer, and Perception layer, as shown in Fig. 1. The Application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed. The Network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data. The

Robin Singh and Jing-Chiou Liou are with the Department of Computer Science and Technology, Kean University, Union, NJ, 07083, USA (e-mail singhro@kean.edu and jliou@kean.edu)

perception layer is the physical layer, which has the actual sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

III. MEDICAL IoT VULNERBILITIES

Modern networks in today's IT Infrastructure are susceptible to many different attacks. The attack of our focus is Denial-Of-Service Attacks (DoS), more specifically Distributed-Denial-Of-Service attacks (DDoS). DDoS attacks involve the use of bots (compromised computers that have some type of malware) or a group of bots (known as a botnet) that is controlled by an attacker who has a Command-and-Control Server (CCS) that allows the attacker to direct the botnets to attack a network. Figure 2 shows how a IoT devices can be hijacked [17]:

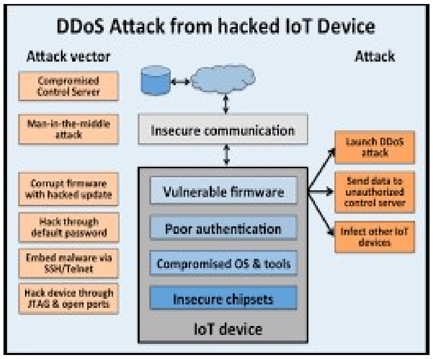
DDoS Attack from hacked IoT Device
Attack vector
Attack
Compromised Control Server
Man-in-the-middle attack
Corrupt firmware with hacked update
Hack through default password
Embed malware via SSH/Telnet
Hack device through JTAG & open ports
Insecure communication
Vulnerable firmware
Poor authentication
Compromised OS & tools
Insecure chipsets
IoT device
Launch DDoS attack
Send data to unauthorized control server
Infect other IoT devices

Fig 2: Attack vectors of IoT device to be used as Botnets[17]

DDoS attacks can be further classified into three categories: Application Layer attacks, Resource Exhaustion attacks, and Volumetric Attacks. IoT networks support both transport layer protocols, UDP and TCP. Therefore, IoT networks are susceptible to flooding attacks such as SYN Flood (exploits TCP protocol) and UDP Flood (exploits UDP protocol). A specific kind of UDP flood attack, called SSDP reflection (one type of DDoS) attack, is explained in [8].

This type of attack is similar to the SYN flood (also known as a half-open attack) that aims to make a server unavailable to legitimate traffic by consuming all available server resources, by repeatedly sending initial connection request (SYN) packets. The attacker is able to devastate all available ports on a targeted device, causing the targeted device to respond to legitimate traffic very slowly or not at all. The UDP Flood is a type of Volumetric Attack that involves a large number of UDP packets flooding a network system, deeming it temporarily unresponsive.

There are a wide range of sensors and actuators used in the environment of hospitals, patient care homes, and the homes of actual patients. Most patients that are debilitated by their health tend to have devices implanted into them or devices that they carry around to support their health. Some of these devices include pacemakers, insulin pumps, hearing aids, sensor-based asthma inhalers. Though many of these devices may seem secure, there are many vulnerabilities existing inside of these devices and sensors.

According to the OWASP Top 10 IoT Risks, the number one risk associated with these devices are default/misconfigured passwords. It has been seen that in the Mirai malware case the IoT devices were hijacked because they were utilizing their generic credentials [7]. Once these devices are hijacked and a hacker gets possession of them, they can easily be used to target a victim server.

The botnet can generate traffic directed back at the server which turns into an intermediary and all devices connected to that server will be reverse broadcasted by the server causing amplification-based DDoS attacks. Amplification based DDoS attacks are generally measured in the volume of traffic generated and the speeds (bits per second). In this case the botnet doesn’t have to be that big to cause problems since it’s not the actual botnet carrying out the attack. Therefore, the attack can be carried out without any consequences on the attacker’s side.

IV. HEARING AID ARCHITECTURE AND SECURITY RISKS

Hearing aids(HA) are one of the common medical IoT devices in healthcare. Hearing aids assist individuals with hearing problems which escalates the sound nearby the surroundings. Recently hearing aid has also been included in the category of IoT because companies are manufacturing smart hearing aids. These smart hearing aids are now capable of utilizing wireless streaming and Bluetooth connectivity [9]. The hearing aids are two-way communication devices which means they can take input from an intermediate node or surrounding and can send some information back to the intermediate node like a cell phone which may either process this information by itself or send it to the cloud or backend server of the physician [13].

The mobile device acts as an intermediate node that is linked to the smart HA using Bluetooth Low Energy. The hearing aid applications are now making it more feasible for patients to connect their hearing aid to other IoT devices like ring bell, refrigerators etc. through If-This-Then-That (IFTTT) applet [13], [14].

The designed applications for these devices make it possible for connecting to your healthcare provider, by just entering a six-digit passcode, who can remotely send out therapies for the patient’s treatment to his hearing aid [10]. Healthcare professionals are the ones who provide this six-digit passcode.

In order to hijack one single hearing aid, the malicious hacker within range may pair up his rogue device and then make some alteration to Hearing Aid modules or binaries. He may later then unpair his rogue device to let authentic user pairs up. Once the authentic user pairs up, he will be using the device with the malformed configuration.

After this malicious configuration, the communication now may rather be going to the victim server instead of the physician's cloud. The IoT devices, which relies on Bluetooth to connect to cell phones provides four types of pairing methods 1) Just Works 2) Out of Band 3) Passkey 4) Numeric Comparison method [11].

From our research, we were unable to find out which exact pairing method do hearing aid manufacturers implement but there is a great explanation of how pairing method selection decision is made by manufactures [11]. To support our hypothesis, we checked out a few consumer experience videos on how HA is paired up to a cell phone and it looks like there is no key shared among both devices [10], [12]. Thus, it must have implemented the Just Works method with the least security. Just Works also implements the ECDH key share in order to enhance security but in order for that key exchange security, the device (HA) itself has to have Display or keyboard with Display [11].

A. Hacking multiple hearing aids scenarios

Although this type of malicious hack can be done when the victim is in range but in order to initiate a DDoS attack where multiple botnets are required, this strategy seems futile. However, following are some of the possible other attack surfaces that can be used in order to hijack number of hearing aids to perform DDoS attack:

- Malicious app connecting to IFTTT cloud
- Malicious firmware update from clinic.
- Malicious therapy installation through remote programming

Malicious/Outdated apps connecting to IFTTT cloud*:* One may download a malicious/unpatched IoT application and integrate it into IFTTT applet in order to make it work with hearing aid. Then this app may read the BLE module of the hearing aid which is stored in the phone and may end up making some changes to the hearing aid itself. The BLE module stores the key that is used to communicate to the hearing aid. Attackers can simply overwrite data in BLE devices.

Malicious Firmware update from clinic: Few manufacturers do not allow the patient to update the hearing aid firmware from mobile apps but instead you need to visit the clinic so that the doctor can update that for you in-person [15]. It is believed that few access controls on client side are implemented by making the physician as the trusted node for the firmware update. Since, hearing aid is implementing Just Works pairing method which in itself is the basic method, there is quiet a possibility that its phone application is responsible for verifying the update if it is actually coming from the trusted manufacturer. If the credentials for the system that physician has in office are default or easy to guess, there is quite a possibility for a malformed update to be pushed for installation every time a patient with hearing aid comes in for the new change.

Malicious therapy installation through remote programming: After pairing with physician's cloud using six digit code, your doctor can send your therapies (aka programs) for your treatment directly to your phone app which HA may utilize for treatment. We were unable to verify if these programs are digitally signed or what protective measures are being implemented in order to secure these program/therapies that are being sent out to the client. In case of credential hijack in a physician's system a malformed therapy can be broadcasted to exploit the hearing aid devices.

Reverse engineering technique, fuzzing attack methodology, can be used by attackers on hearing aids to better understand how they communicate. In Bluetooth enabled devices, it is quite a possibility where an attacker can use it to overwrite or craft a malformed packet in the device that may cause the BLE device to misbehave [11].

If the packets are malformed, they can contact the cell phone by saying "Hey phone, send these packet X number of times to victim 10.0.0.55" or a forged IP address can be used by hearing aid to send the large response to the legitimate victim server as it happened in the SSDP flood scenario. Figure 3 demonstrates how an attack based on scenario can be performed by hacker.

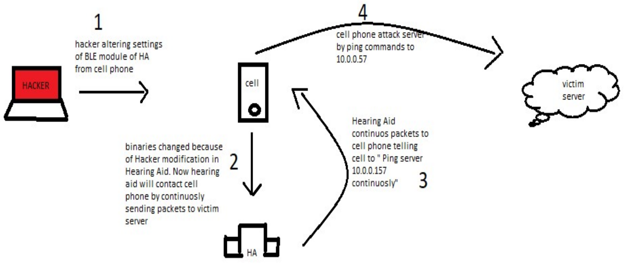
1
hacker altering settings of BLE module of HA from cell phone
HACKER
cell
4
cell phone attack server by ping commands to 10.0.0.57
victim server
binaries changed because of Hacker modification in Hearing Aid. Now hearing aid will contact cell phone by continuosly sending packets to victim server
2
Hearing Aid continuos packets to cell phone telling cell to " Ping server 10.0.0.157 continuosly"
3
HA

Fig. 3 shows how scenario-based hijack for Hearing Aid can be done

B. Hearing Aid Conclusion

Hijacking hearing aids and turning to botnets is quite a difficult process. Since it is only discoverable for several minutes, the hacker needs to be within range in order to pair it up with his own device [16]. Then he may be able to make changes to the hearing aid by performing fuzzing attack and then later unpair so that the original user can utilize the malformed Hearing Aid. However, as mentioned earlier, this strategy isn't usable in case of performing DDoS attacks. A single hearing aid is incapable of generating such a volume to take down the entire server. In order to hijack a number of hearing aids, a single manufacturer can be targeted and its hardware vulnerabilities can be learnt through reverse engineering process. Since, hearing aid itself is compatible with the Just Works pairing method of Bluetooth Low Energy, there is no interface on the hearing aid to generate keys or verify the authentication of updates.

V. PACEMAKER ARCHITECTURE AND SECURITY RISKS

Pacemakers are medical devices, classified in the medical IoT category. These devices are fault tolerant architectures and fail safe, they rely on multiple computations and redundancy to perform its job. The role of a pacemaker is to keep the heart beating whether it falls below the minimum threshold or the maximum threshold for beats per minute. These devices have a lot of security in mind because of how important they are. If a pacemaker malfunctions, it results in a life-or-death situation for the person wearing it. As we know, no device in this world, especially IoT devices are secure therefore there are always attack vectors that play a huge role.

The pacemaker needs to be paired with Bluetooth or radio frequency in order to collect the data. In order to pair with the pacemaker, pacemaker's serial number is used to pair the device to the app/home monitor (discussed later). If there are ten pacemaker patients sitting in a room with ten home monitors, Patient A's pacemaker will only send data to its home monitor. Cross talk is not possible since the serial number is used to pair up the both devices. As was noted in the section above, Bluetooth hijacking may become a reason to intercept all of the data being sent from the pacemaker to the home monitor. But in order to alter setting of pacemaker the attack surfaces need to be explored. Following are the few vectors that are associated with pacemaker:

A. Lead Issues:

The purpose of the pacemaker's leads is to convey the stimulus pulses from the pacemaker to the heart as well as the intrinsic cardiac signals from the heart to the pacemaker [4]. Lead fracture or failure can lead to issues with under-sensing and over-sensing, which will ultimately result in the pacemaker collecting erroneous data that the doctor will use to treat the patient [2]. Since it is a hardware-based issue, further research needs to be done to verify if any alteration in the settings may impact the lead performance.

B. Home Monitor/Remote Monitor:

The Pacemaker's Home Monitor, also known as Remote Monitor, is another surface that can ultimately be categorized as an attack surface. Remote Monitoring system is optional to have with pacemaker. It records data on heart rhythm (heart rate, atrial and ventricular arrhythmias), device performance (battery life, lead function), therapies administered by the device (anti-tachycardia pacing [ATP] and ICD shock), and physical activity (steps taken per day) [1]. The businesses that produce these remote monitoring systems play no role in turning the pacemaker on/off, changing settings or reprogramming/updating the device. Thus, the pacemaker cannot be hijacked by utilizing a home monitor.

Encryption techniques are implied in order to secure the transmission between home monitor and pacemaker. The use of an asymmetric algorithm to send information from pacemaker to health monitor is not feasible because of the limitations caused by Pacemaker's size and design [3]. As a result, a time-based one-time password is utilized, which produces a password depending on the time passed and a predetermined secret key.

In the past, the home monitor from Medtronic has a flaw identified as CVE-2019-6538. According to CVE MITRE, which claims that the communication (telemetry) protocol used by the monitor and programmer (discussed later) doesn't perform authentication and authorization. Any nearby attacker can inject, replay, and alter memory data in the communication protocol. The alteration of memory in the pacemaker through the home monitor is not possible because it is only a one-way connection. Additionally, some home monitoring systems employ subpar VPN while sending data to a cloud used by doctors.

C. Mobile App:

The same manufacturers who are manufacturing pacemakers and home monitoring systems have developed mobile applications as an alternative to the home monitoring system. It performs the similar operations as home monitoring systems. It also plays no role in changing settings, turning pacemakers on/off, and providing therapies. The sole purpose for this application is to take data from a pacemaker on a fixed schedule and then transmit this data to the physician's cloud storage for him to review. This app also utilizes Bluetooth low energy to communicate with the pacemaker to fetch its results.

In order to pair with the pacemaker, pacemaker's serial number is used to pair the device to the app. This way the a pacemaker one will always send data to its mobile app. No matter if pacemakers 2, 3, or 4 are present with their own mobile app. Similar to the home monitoring system, the schedule of transmitting data to the app is programmed. Both home monitor and app provide functionality for which the user can use to send data right away.

Although Bluetooth hijacking or MAC address spoofing can be done to send exploited data to the app or home monitor, since the schedule is fixed for transmitting the data to the cloud, it is not feasible to conduct a DDoS attack by using pacemaker as the botnet. Theoretically the pacemakers can never conduct a DDoS attack by acting as a botnet (where devices send hundreds of packets at the same time).

D. Patient Programmer:

The fourth attack surface can be the patient programmer which physicians have in their office in order to change settings, provide therapies, or scheduling intervals to send data to the cloud. The connection between a pacemaker programmer and a pacemaker is two-way because pacemaker can upload its data to programmer and programmer may alter the settings in the pacemaker, provide therapies and reconfigure the scheduling time to send data with the help of intermediary node to the cloud. Through RF technology, pacemaker's serial number is used as a token key to initiate the session. Once the session is established there is no other authentication done to recognize if this is the valid pacemaker or Programmer. Since this programmer device is not password protected, it can be used by someone who has physical access to it. It is likely that if this patient programmer itself is hacked, any incoming patient for their treatment may be tailored with malicious settings or make any incoming pacemaker to send data to a specified address upon X intervals.

VI. MITIGATION STRATEGIES

The ultimate goal for any DDoS security attack is to hijack a system to perform something malicious. In our research we have focused specifically about DDoS attacks and their impacts on medical IoT Devices. The most important aspect in security is prevention but we know that it is not always possible. So if prevention doesn't take place, mitigation does. The goal of any mitigation strategy is to reduce the severity of any attacks and in our case the goal is to reduce the chances of medical IoT devices getting hijacked and turned into bots to perform a DDoS attack. To that aims, we have developed several mitigation methods based on the best practices.

The number one mitigation strategy for hearing aids would be to enforce some cryptographic keys in order to initiate a connection with middle node. The vendors are strongly encouraged to restrict the use of misconfigured/default credentials. As mentioned before, according to OWASP Top 10 vulnerabilities for IoT Devices, the number one vulnerability is default/misconfigured passwords. The patient portal/system to send therapies and updates to hearing aids needs to be protected in order to restrict any attacker to use them in order to reconfigure multiple hearing aids at once. But in order to reconfigure multiple hearing aids at once, sophisticated reverse engineering techniques are needed in order to alter the behavior.

In regards to the pacemaker, through our research, we found out that it is not possible to convert the pacemakers into botnets to conduct a DDoS attack because intermediate devices like home monitor and pacemaker app are only one-way communication device. Since, there has not been any information regarding architecture or general information provided for home monitor and phone apps, it is quite difficult to analyze what security vulnerabilities these devices possess or if they can be hijacked as a botnet to conduct a DDoS.

There can still be some recommendations to add more security layers to prevent pacemakers from being exploited. It is highly recommended that the manufacturers do start to modify the architecture of the pacemaker to allow asymmetric encryption when talking to home monitor, app, or the programmer so that it will be difficult for hackers to break the encryption and view the data in motion.

Secondly, it has been noticed that patient programmers can be bought online from sites like eBay [3]. This sale does need to be restricted in order to stop hackers from learning more about the architecture or connecting to the pacemakers in range.

In the study, it has also been discovered that emergency functionality can be used to record and send the data immediately if a patient with pacemaker feels uncomfortable. Due to the less sources available, it is assumed that manufacturers do reduce the number of manual record and transmission so that no hacker in the range may conduct mac address spoofing to send exploited data to the home monitor or app. If this feature is not already embedded, it is highly recommended for the manufacturer to do so.

VII. CONCLUSION

It has been noted in the research that medical IoT devices like hearing aids and pacemakers uses Bluetooth technology in order to communicate with the server, it requires an intermediary node (connected to the Internet) to send the collected data to the physician's cloud/server. Although, there is a possibility of attacking these Bluetooth enabled devices, it is not feasible to hijack these devices in large number to initiate DDoS attack unless the associated device (app, vendor portal or programmer) is capable of two-way communication and contains vulnerabilities. Even if such vulnerabilities do exist in intermediary devices, a sophisticated level of reverse engineering and altering skills are required in order to make such a large change in the Bluetooth medical devices. Further research is needed to better understand the architecture and role of intermediary nodes if such reverse engineering tactics can be employed to make such alteration.

REFERENCE

[1] L. Rosman, L. E. Rosenfeld, M. L. Johnston, & M. M. Burg, Remote monitoring of implanted cardiac devices: A guide for patients and families. *Pacing and Clinical Electrophysiology, 41(9), 1224–1228.* https://doi.org/10.1111/pace.13456

[2] T. Liaquat,, Muhammad et al. Pacemaker Malfunction. Statpearls Publishing. https://www.ncbi.nlm.nih.gov/books/NBK553149/

[3] S. Das, G. P. Siroky, S. Lee, D. Mehta, & R. Suri, Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm, 18(3), 473–481.* https://doi.org/10.1016/j.hrthm.2020.10.009

[4] G. I. Alkady, I. Adly, H.H. Amer, & T.K. Refaat, Mitigation of Soft and Hard Errors in FPGA-Based Pacemakers. *2018 13th International Conference on Computer Engineering and Systems (ICCES).* https://doi.org/10.1109/icces.2018.8639480

[5] P. Sethi, S. R. Smruti, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, Vol. 2017. Pp. 1-25. `https://doi.org/10.1155/2017/9324035

[6] IoT devices (internet of things devices) https://www.techtarget.com/iotagenda/definition/IoT-device

[7] What is the Mirai Botnet? https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[8] Y.-J. Lee, H.-S. Chae, and K.W. Lee, Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices, Journal for Control, Measurement, Electronic, Computing and Communications, Vol. 6, Issue 1, pp. 127 – 136, Feb. 2021.

[9] K. Panagiotis, and D.D. Koutsouris, A (Lack of) Review on Cyber-security and privacy concerns in Hearing Aids, proc. 2018 IEEE 31st International Symposium on Computer-Based Medical System (CBMS), DOI:10.1109/CBMS.2018.00046

[10] How to pair Signia gearing aids to an iPhone or iPad https://www.youtube.com/watch?v=1ISLz0C64lY

[11] A. Barua, et al. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey, IEEE Open Journal of the Communication Society, Vol. 3, pp. 251 – 281, Feb 2022.

[12] How to pair Bluetooth compatible hearing aids to an Android smartphone https://www.youtube.com/watch?v=XO48NylDG7U

[13] Oticon On App | How to use with your Oticon More Hearing Aids! | Applied Hearing Solutions https://www.youtube.com/watch?v=WuUOcwu1qM4

[14] Oticon Bluetooth® hearing aids and IFTTT - Craft Your Own Connections https://www.youtube.com/watch?v=UdYIDhn7Cuo

[15] Oticon Firmware Updater https://www.youtube.com/watch?v=Sm9H2jgo4XM

[16]Can my Bluetooth Hearing Aids get Hacked? https://www.valuehearing.com.au/news/can-my-bluetooth-hearing-aids-get-hacked#:~:text=Through%20secure%20wireless%20technology%20and,this%20connection%20is%20not%20possible

[17] DDoS attacks using IoT devices follow the Manchurian Candidate model https://www.networkworld.com/article/3128372/ddos-attacks-using-iot-devices-follow-the-manchurian-candidate-model.html

[18] Hasan et al. Solutions of common challenges in IoT. *IOSR Journal of Computer Engineering. Volume 19, Issue 5, Ver. V (Sep.-Oct. 2017), PP 57-6*