Security for Implantable Medical Devices with Wireless Connections: using Multi-Factor Authentication Approach

G.C.Sathish[1], B.R.Leelavathi[2], Bindu.M.Raju[3]

[1]Professor
[1,2,3]School of Computing and Information Technology,
REVA University, Bengaluru, India
[1]sathish_gc@reva.edu.in, [2]leelaramachandras@gmail.com, [3]bindumanjunath08@gmail.com

Article Info
Volume 83
Page Number: 5379-5383
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *16 May 2020*

Abstract

Modern wi-fi enabled implantable medical gadgets (IMDs) began to be extensively delivered to scientific customs in early 2000s, when devices such as cardiac implants, insulin pumps, and neurological implantable pulse generators (IPGs) began with features like wi-fi controls and monitoring functions. The improvement of the wi-fi gadgets has modified the panorama of security in the clinical area. There are many wireless medical device threats like denial of service, modifying data, tracking the patient. Securing these implantable clinical devices against assault without compromising affected person health requires balancing protection and privacy objectives with traditional desires including safety. Moreover, the modern-day IMDs resource delivery of telemetry for far off monitoring over lengthy-variety, excessive-bandwidth wi-fi links, and growing gadgets will communicate with different interoperating IMDs. Wireless manipulate features permit attackers to govern IMD settings from past the instant place of the affected person, whilst networked IMDs are at risk from attacks originating anywhere in the world.

Keywords: *Security, Implantable medical device One Time Password, Email Tokens, Multi Factor Authentication, Username, Password*

1. Introduction

Implantable medical device system examine and treat physical conditions within the body. These gadgets - consisting of a pacemaker, cardiac defibrillator , drug transport systems, and neurostimulators - can assist deal with many ailments, which includes coronary heart disorder, diabetes and Parkinson's disorder. Wireless connectivity enables IMDs to communicate with specific external devices such as device systems, base stations and external sensors[2]. Malicious hackers can attack easily due to cyber security failures. Most of the people are familiar with the most common types of computer breaches – which are caused by computer hackers, computer malware, viruses and the loss or theft of laptops containing confidential data or records. The concern about security also extend to other systems installed on standard clinical devices, which have become more cultured and often dependent on refined software and greater automation. Wireless controlling factor allow attackers to compromise IMD settings beyond the patient's area, connected IMDs (i.e. those that are associated with internal medical centre networks, that are vulnerable to attacks from anyplace in the world. Wireless IMDs, as they are now used in medicine, present many risks. The connection between IMD and the channel or system resource can be affected and, if the signal waves are not secured by authentication procedure, the attacker can gather or modify the data, as much as possible while being present in remote areas. Although protected but authentication, which does not exist in many existing devices, the nearness and example of such signals can provide profitable data to the attacker[1].

Appropriate protection of scientific devices ought to make sure dependable, secure communique and persisted functionality even as maintaining patients' protection, confidentiality, and information integrity. Though there is almost typical settlement on the significance of security for personal fitness information and electronic fitness records, there is confrontation over the safety requirements for medical devices [3].

2. Related work

At the recent Black Hat information protection conference, researchers established how the Care link 2090 pacemaker, alongside the enterprise's insulin pump, might be hacked.

First, they warned all people with an implanted tool to go away the room. Then they disabled an insulin pump. A hacker near a patient may want to replica the tool's radio frequency indicators, after which play them returned later to deliver insulin whilst it isn't wished– potentially main to dangerously low blood sugar. They additionally hacked a gadget that doctors can use to program a affected person's pacemaker. The hack may be used to surprise a person's heart, or to withhold a shock whilst it's needed. The first pacemaker hacks emerged about a decade in the past. But the modern variant at the terrifying subject relies not on modifying radio commands, as many previous assaults have, however on malware hooked up immediately on an implanted pacemaker.

For almost two years, specialists Billy Rios of security firm Whitescope and Jonathan Butts of QLED Secure Solutions have gone to and fro with pacemaker Medtronic which makes Carelink 2090 Pacemaker developers and other important hardware that scientists state contain possibly perilous vulnerabilities. Over 2.6 million of insulin pumps and pacemakers were implanted in United states and trials were made as these devices increased the survival rate.

The coronary heart generates electrical signals to induce heartbeat. The coronary heart's electric device can turn out to be defective due to getting older or different reasons, leading to as decrease heartrate(bradycardia). Such illnesses may be treated the use of pacemakers, which are implantable medical devices that generate the electric alerts required to keep the heartbeat at a healthful rate. Hence pacemakers are protection-critical gadgets.

The mechanism of the pacemaker revolves around sensing and signaling of electrical pulses. A DDD mode pacemaker has leads connected to the proper atrium and proper ventricle.

Latest years have seen growing popularity of cybersecurity hazard in implantable clinical devices and extra commonly during medicinal drug. The FDA issued its first safety communique concerning risk, warning doctors about the safety defects in Hospira outside drug infusion pumps in 2015 . In 2016 Johnson & Johnson released a caution about the defects of their OneTouch implantable insulin pump device following e book via manner of impartial protection research company Rapid7, placing the equal antique for responsible disclosure of the vulnerabilities. Recently, it was shown that security assaults can be performed on wireless communication, which lead to dysfunction of the insulin pump system. Body coupled communication technology is used to reduce the range of transmission and consumption of power during exchange of data[4].

Unapproved access to the IMD Having caught the PIN of the IMD, a foe can completely get to the IMD segments to play out a few modifications that could hurt the patient's wellbeing, for example, a modification on the treatment settings. In in the wake of acquiring an unapproved get to, it gets conceivable to stop the infusion of insulin and lead to a high glucose level in the patient's body. Having accessed the IMD, a foe could likewise execute unapproved orders to change the IMD firmware, erase information put away in the IMD, or even debilitate it[4].In the decade of 90's, six deaths were caused in a row because of the Therac25 incident, which was due to assembling and programming error. The first failure happened when a 21 year old expired due to short circuit with the usage of cardiac defibrillator[7].

Much less accountable became the 2016 disclosure by means of safety research company Medsec and investment company Muddy Waters concerning security defects in the St Jude Merlin Home pacemaker tracking machine, which gave upward thrust to a lawsuit and raised extreme moral questions. This event led to an remarkable FDA don't forget – the primary related to cybersecurity of the St Jude pacemaker machine in 2017 consisting of a software program update to fix the troubles. Recent ransomware assaults on health center networks, defusing critical clinical devices and compromising patient statistics, also definitely reveal the dangers of uncertain clinical pc structures and underscore the significance of enhancing security.

Wi-fi implantable devices, as presently used in clinical practice, show off many flaws. Communique a few of the medical devices and a base-station or programmer device can be obstructed and, if the alerts aren't included via encryption and/or authentication protocols, an aggressor can gather or regulate the records, likely while located hundreds of meters away. Even supposing blanketed with the aid of secret code, which many available gadgets are not, the mere existence and sample of such signal waves can offer data that might be treasured for an attacker.

The bottom-station or programmer can also be the objective of intrusion; its communications with other gadgets on a wi-fi(or over the internet)may be amassed and adjusted, and the tool can be undermined thru physical or far flung introduction of malicious code. This latter trouble is of significance as IMDs are more and more created to interface with purchaser e-gadgets which include smartphones and pill computer system, opening up the opportunity of malware focused on the client tool and thereby having access to programmer packages that control the IMD. Potential assaults are not restrained to advanced structures, with analog sensor and effector additives of IMDs being at risk of spoofing attacks.

The results of those vulnerabilities, ought to they be misused, are fluctuated and most likely significant. stealing of knowledge and denial of treatment are attainable across most wirelessly connected IMDs, with battery-depleting assaults being notably possible to conduct and harming to patient health. internal organ implants and deep-rooted hormone pumps may be modified to induce cardiac rhythms, or deliver associate hormone bolus, that will be fatal . medical specialty implants, usually having additional advanced however less life-basic capacities, are defenseless to assaults with an outskirt shift of outcomes together with affecting the patient’s considerations and conduct. This latter risk has raised troublesome legitimate and moral questions, notably relating to patient autonomy.

Modern implantable devices normally has personal statistics saved in their memory. Basic info which include touch information for the affected person’s health practitioner, date of delivery, and name would all be able to be utilized by an aggressor to interact in social planning and identification robbery. More technical record, inclusive of the stimulation settings of the IMD or the rate of battery defuse, can be used to deduce info of a affected person’s circumstance, which an aggressor should make use of to facilitate assaults depending on precise pathological states . Also regarding from a security angle is the biometric records that these gadgets are accumulating in high numbers. Closed-loop implantable devices use physiological records collected by means of sensors to prevent electric stimulation or drug delivery through effector additives, however these statistics can be profitable to attackers who want to decide information of a affected person’s pathology, or even potentially get entry to statistics about patient’s mind-nation, as validated by means of

Martinovic and co-workers, who correctly hired aspect-channel attacks against a non-invasive mind-system interface machine and thereby found out individuals’ personal records.

3. Methodology

Medical centers are developing into digital environments, industries are developing and introducing Wi-Fi medical devices, and e-gadgets are beginning to gather health records on individuals. These data are stored in medical repositories and based on these day to day data received by monitoring the patient are also recorded and stored. As the medical implantable devices are controlled wireless, the data can be at threat to the patient as there may be loss of information or any modification made to the implantable device. To ensure the prevention of these attacks, the MFA is one of the key techniques.

Multi-Factor Authentication is a security device that verifies a consumer’s identification by means of requiring multiple credentials. It is a vital element of identity and access management. Rather than simply inquiring for a username and password, MFA calls for different extra-credentials, consisting of a code from the consumer’s phone, the solution to a security question, a fingerprint, or facial popularity. The credentials can be of these categories:

1. Knowledge: These are information that a person is aware of, which include security key or answers to personal questions.
2. Assets: These are things that an individual has, which include a physical photo-ID cards, cellphone, physical keys, digital authenticated code, a hardware USB dongle (pen drives) , or virtual secured keys.
3. Physical Characteristics: It is biometric information which includes, things like fingerprint sensing, retinal/iris detection, facial features, bone density and DNA.

The functionality of our system is described below as per the diagram. As the user opens the website, a login page is opened where he/she has to enter their respective credentials (i.e.) the username (email ID of the user) and password. Now, the system checks the database for the username and password, verify and validate with a popup for the current status. The proceed button on click will redirect the user to the page which asks the user to select yes or no for receiving one time password(OTP) on the registered mail. If yes, then a time based one-time password is sent to the user on his/her mail ID.

The one-time password algorithm generates alphanumeric characters or random numbers and this one-time password is sent to the respective mail Id. The user enters the received token and the system checks and validates with a popup for current status. The proceed button onclick will redirect the user to the page which asks the user to select yes or no for receiving one time password to the registered phone number.

The one time password algorithm generates random four digit numbers which is valid for time period of two minutes and this is sent to the registered phone number. The user enters the received SMS tokens and the system verifies and validates and then user is given to access the website. The users may be patients or doctors where they can communicate and view the medical records.

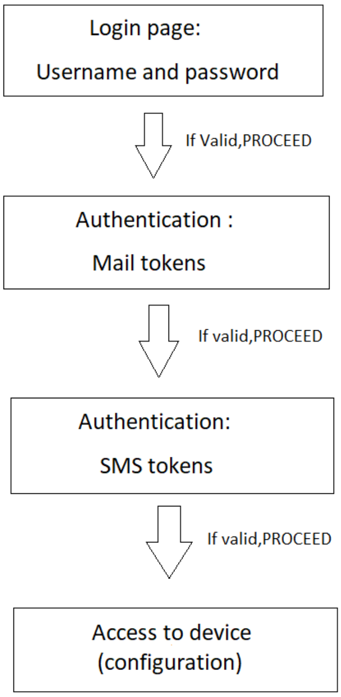
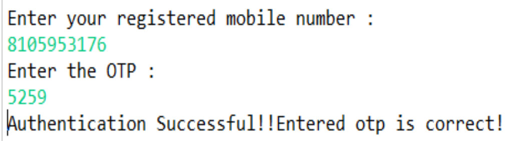


Figure 1: Flow of control Diagram

4. Results and Discussions

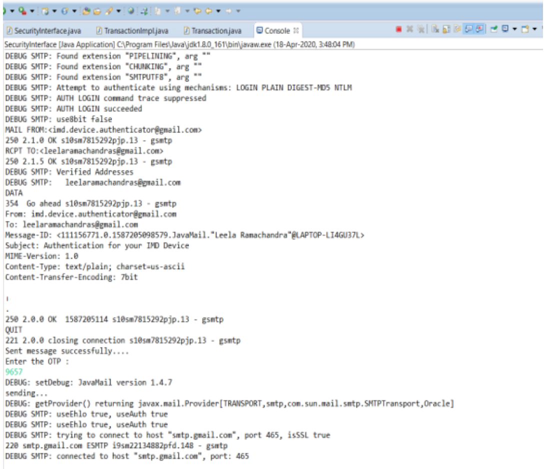
Multi-factor authentication, requires the authentication process to include verification of factors by taking the input from users in form of - something a user already knows (username and password) ,something a user possesses(time based one-time password sent to the user's mail ID). The user, using the user interface, enters the user credentials i.e. (username and password). Here, the username entered by the user is their mail ID which is already stored in a database by the admin. The system validates the credentials by comparing the credentials present in database with the user entered credentials. Once the first step of authentication is successful, then the user can go for the second step of authentication, via an email-token. The admin now sends the one-time password to the registered mail ID.

The system now redirects the user to a page where he/she can enter the received one time password. The system now validates the one time password. If a match is found among the user entered one time password and the one sent from the admin end, then the user is allowed to access the settings and configuration of their implantable wireless medical device.



```
Enter your registered mobile number :
8105953176
Enter the OTP :
5259
Authentication Successful!!Entered otp is correct!
```

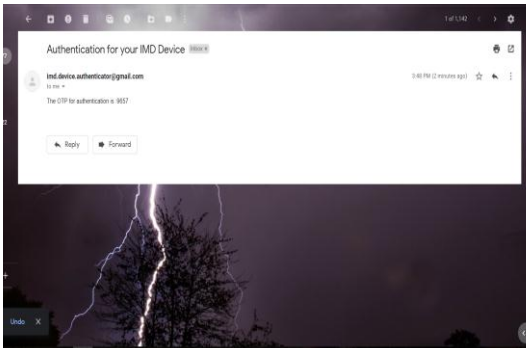
Figure 2: This figure shows the validation of one-time password which is sent to the registered phone number of the user



```
SecurityInterface [Java Application] C:\Program Files\Java\jdk1.8.0_161\bin\javaw.exe (18-Apr-2020, 3:48:04 PM)
DEBUG SMTP: Found extension "PIPELINING", arg ""
DEBUG SMTP: Found extension "CHUNKING", arg ""
DEBUG SMTP: Found extension "SMTPUTF8", arg ""
DEBUG SMTP: Attempt to authenticate using mechanisms: LOGIN PLAIN DIGEST-MD5 NTLM
DEBUG SMTP: AUTH LOGIN command trace suppressed
DEBUG SMTP: AUTH LOGIN succeeded
DEBUG SMTP: use8bit false
MAIL FROM:<imd.device.authenticator@gmail.com>
250 2.1.0 OK s10sm7815292pjp.13 - gsmtp
RCPT TO:<leelaramachandras@gmail.com>
250 2.1.5 OK s10sm7815292pjp.13 - gsmtp
DEBUG SMTP: Verified Addresses
DEBUG SMTP:   leelaramachandras@gmail.com
DATA
354  Go ahead s10sm7815292pjp.13 - gsmtp
From: imd.device.authenticator@gmail.com
To: leelaramachandras@gmail.com
Message-ID: <111156771.0.1587205098579.JavaMail."Leela Ramachandra"@LAPTOP-LI4GU37L>
Subject: Authentication for your IMD Device
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

!
.
250 2.0.0 OK  1587205114 s10sm7815292pjp.13 - gsmtp
QUIT
221 2.0.0 closing connection s10sm7815292pjp.13 - gsmtp
Sent message successfully....
Enter the OTP :
9657
DEBUG: setDebug: JavaMail version 1.4.7
sending...
DEBUG: getProvider() returning javax.mail.Provider[TRANSPORT,smtp,com.sun.mail.smtp.SMTPTransport,Oracle]
DEBUG SMTP: useEhlo true, useAuth true
DEBUG SMTP: useEhlo true, useAuth true
DEBUG SMTP: trying to connect to host "smtp.gmail.com", port 465, isSSL true
220 smtp.gmail.com ESMTP i9sm22134882pfd.148 - gsmtp
DEBUG SMTP: connected to host "smtp.gmail.com", port: 465
```

Figure 3: This shows the verification of the one time password sent to the registered mail ID of the user

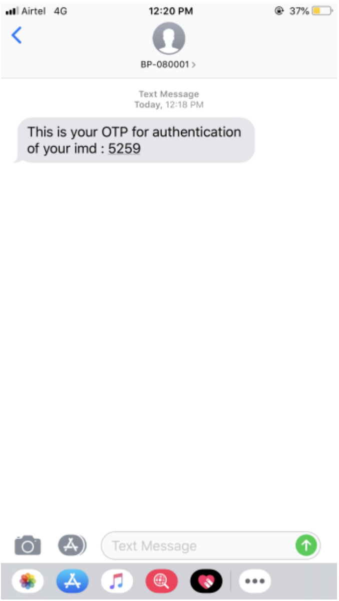


Authentication for your IMD Device

imd.device.authenticator@gmail.com
to me
3:48 PM (2 minutes ago)

The OTP for authentication is 9657

Figure 4: One-time password sent to registered mail.



BP-080001

Text Message
Today, 12:18 PM

This is your OTP for authentication of your imd : 5259

Figure 5: One-time password sent to registered phone number

5. Conclusion and Future Scope

Two-factor authentication is essential for ensuring a proper level of access to user identity verification. If an attacker manages to compromise credentials, this records gained will not be enough to get admission to an account besides. With MFA enabled, it turns into nearly impossible for hackers to pass all authorization steps. Once they input accurate login details, additionally they need to compromise biometrics or intercept an OTP which calls for more value and effort to behavior a success attack.

The proposed system aims to bring out a secured access for the patients and the doctors ensuring prevention from attacks. This authentication approach can be further enhanced by implementing more factors such as:

- Fingerprint: A form of biometric authentication, fingerprint authentication robotically compares a consumer's fingerprint to a stored fingerprint template on the way to validate a consumer's identity. As everyone has unique fingerprints, fingerprint acts as a unique factor, makes impossible to guess and difficult to modify or fake.
- Iris recognition: It is an automatic technique of biometric identity that uses pattern recognizing technique on video photographs of the irises of an individual's eye, whose complicated random styles are precise and can be visible from a long way.
- Hardware tokens: It is an approach to user authentication that depends on a particular physical device (such as a token) held by an authorized user. The device generates a unique and temporary cryptographic code that must be input by the user as a security key in addition to a password, to gain access to a computer resources.

Acknowledgement

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along the completion of our project.

We respect and sincerely thank G C Sathish for this support and guidance which made us complete the project duty.

References

[1] Laurie Pycroft & Tipu Z. Aziz. "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks"2018, Expert Review of Medical Devices, 15:6, 403-406, DOI: 10.1080/17434440.2018.1483235

[2] Daniel Halperin, Thomas S.Heydt-Benjamin,Kevin Fu, Tadayoshi Kohno,and William H Maisel "Security and Privacy for Implantable Medical Devices" Jan-Mar 2008 Vol.7,No.1 January-2008

[3] William H.Maisel,M.D,M.P.H, and Tadayoshi Kohno,Ph.D." Improving the Security and Privacy of implantable Medical Devices".

[4] Nourhene Ellouze, Mohamed Allouche, Habib Ben Ahmed, Slim Rekhis and Noureddine Boudriga "Security of implantable medical devices: limits, requirements, and proposals" 2014 Published online in Wiley Online Library (wileyonlinelibrary.com), Nov 29, ; 7:2475–2491 © 2013 John Wiley & Sons

[5] Patricia AH Williams, Andrew J woodward "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem" 2015 Published in Medical Devices: Evidence and Research, Jul 20, Australia 2015: 8 305-316 ©2015 DovePress.

[6] Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks" 2014 IEEE Symposium on Security and Privacy, May 18-21, San Jose, CA, USA, 978-1-4799-4686-0 ©2014 IEEE.

[7] Heena Rathore, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani "A review of security challenges, attacks and resolutions for wireless medical devices" 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Jun 26-30, Valencia, Spain, 978-1-5090-4373-6 ©2017 IEEE.

[8] Aliya Tabasum, Zeineb Safi, Wadha AlKhater, Abdullatif Shikfa "Cybersecurity Issues in Implanted Medical Devices" 2018 International Conference on Computer and Applications (ICCA), Aug 25-26, Beirut, Lebanon, 978-1-5386-4372-3 ©2018 IEEE.

[9] David J. Slotwiner, Kevin Fu, Andrea M. Russo, Mary N. Walsh, George F. Van Hare "Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians" 2018 Proceedings of the Heart Rhythm Society's Leadership Summit, Jul 2018, Vol 15, No 7, 1547-5271 ©2018 Elsevier Inc

[10] Carmen Camara, Pedro Peris-Lopez, Juan E. Tapiador "Security and privacy issues in implantable medical devices: A comprehensive survey" 2015 Journal of Biomedical Informatics, Apr 24, 55 (2015) 272–289, 1532-0464 ©2015 Elsevier Inc.