SECURITY VULNERABILITIES AND MITIGATION CHALLENGES IN IOT BASED HEALTHCARE SYSTEMS

Garima Saini[1], Suneel Prasad[2]

[1,2] Symbiosis Centre for Information Technology
Symbiosis International (Deemed) University, Pune, India
Email: [2]suneel@scit.edu

Abstract

Internet of Things (IoT) is the term for a technology that is connecting physical objects and devices over the Internet, making these 'things' capable of exchanging data without any human intervention. This data exchange takes place via communication channels like Bluetooth, Wi-Fi, GSM, ZigBee etc. Healthcare industry has been going under complete digital transformation with the help of this technology. Healthcare professionals are now better connected with their patients via smart devices over the Internet. There are numerous applications of this technology that are making the lives of patients better by helping the healthcare professionals to monitor and treat them more efficiently than ever before. However, with the technological advancements for the medical world, not enough commensurate information security defense mechanisms have paced up. This has given rise to the challenge of securing confidential data of patients from unauthorized disclosure. For cyber attackers this data is more valuable than someone's credit card data. The reason being Electronic Health Record (EHR) contains not only the credit card number, but also address, employer and insurance information. Attackers can use this information to open a new credit card in the victim's name, take bank loan or even get high priced narcotics from medical insurer of the victim. Attacks on healthcare applications have increased manifold in the last few years. The purpose of our research is to conduct an analysis of how IoT has been implemented in the healthcare infrastructure of India and what are the challenges related to information security. The focus area of this research are the vulnerabilities of IoT based healthcare systems and threat vectors that the attackers are exploiting. In this paper, we attempt to answer questions like what are the motivating factors for cyber-attackers behind attacking healthcare applications, how are the medical hardware and software vulnerable to IoT based risks, what are the major types of attacks on such systems and how can the medical fraternity manage and mitigate IoT risks in healthcare sector. This research is primarily based on Secondary data with the methodology being comprehensive Systematic Literature Review (SLR). Relevant research papers were reviewed thoroughly, research findings of other researchers, business reports, articles etc. have been referred. Based on our findings, we attempt to propose some strategical solutions that can be used by the management of healthcare organizations to minimize attacks and their impact on critical systems.

Key words: IoT in healthcare, data privacy, security threat vectors, vulnerabilities, risk mitigation, controls, smart healthcare

Introduction

Internet of Things (IoT) can be defined as the network of electronic devices that are capable of exchanging data over the internet via machine-to-machine (M2M) communication protocols. It has connected billions of devices, making the world 'smart'. This technology has evolved rapidly in the recent times thanks to Internet availability, cloud technology and micro services evolution. IoT has been instrumental in bringing automation across various industries like manufacturing, transportation, media and entertainment, chemical and petroleum, pharmaceutical industry etc. Healthcare industry, in particular has experienced tremendous digital transformation as the medical devices are connected over the Internet using this technology. Real-Time Remote patient monitoring and reporting, smart tracking and maintenance of medical equipment, smart health monitoring wearables, ingestible health sensors are few of the numerous examples of IoT based healthcare applications. Apart from directly improving the patient care, IoT is also being used in better data management. Healthcare providers are now able to process large volumes of patient data with much ease and reliability. The data can now be stored in low-cost cloud or archival storage and further IoT applications can even run predictive analysis on the data. According to a study, a rise to $534.3 billion has been projected for IoT technology in the healthcare market by 2025. (GrandViewResearch, 2019)

While IoT has brought revolutionary development in patient care, it has also posed some serious information security challenges. Most of the data that is collected, processed and transmitted in the smart health applications falls in the category of Protected Health Information (PHI) or Personally Identifiable Information (PII). Electronic Health Record (EHR) contains vital information like credit card number, phone number, health insurance information etc. which are targeted by cyber attackers. This paper presents an analysis of the vulnerabilities of IoT based healthcare systems, types of attacks and security control mechanisms in the healthcare industry.

Related work

Classification of IoT based Healthcare applications

Quite a lot of research has been done for understanding the vast span of IoT based healthcare applications. These applications have been classified on parameters like users' age, underlying technology etc.

Patient/user's age-wise classification

IoT based healthcare applications can be classified on the basis of user's age to understand the depth of innovation and advances of services in providing quality care –

Toddlers – Applications like Mimo by Boston startup Rest Devices monitor the respiration, skin temperature, body position and sleeping and activity levels of infants through an imbedded sensor. The collected data can then be tracked on a computer or mobile device.

Kids – iSwimband application is an anti-drowning wearable system that assists in personal aquatic safety. Sleep monitoring systems are also available for kids that track different parameters like blood pressure, body temperature, movement of the body etc.

IoT for Chronic care – Pacemakers, defibrillators and neuro stimulators are used for patients suffering from chronic diseases.

The IoT technology is also being employed in applications such as personal emergency response systems (PERS), motion detection and body motion reconstruction etc. Monitoring during surgery, healthcare mobility aids including wheelchairs and stretchers are yet other applications. (Yeole and Kalbande, 2013)

Based on the architectures of the medical and healthcare IoT systems

Devices can be classified as following– (Anandarajan and Malik, 2018)

Wireless Implantable and Wearable Devices – Internal signals of body are collected by these devices and are then transmitted to an external device. From the medical device, data is transferred to a smart phone, laptop or computer for further analysis by the user. Wearable watches from Fitbit is example of a wearable medical device.

Wireless Emergency Response Devices – These devices are used to track the patient's geographical location and health condition. The data collected from the patient's sensors is then sent to an ambulance base station. Life Alert and Qmedic Medical Alert Bracelets are examples of this class of medical devices.

Wireless Medical Adherence Devices – These devices are used to ensure that the patients, specially the elderly and people with cognitive limitations, follow the medication routines as prescribed by the doctor. E-Pill medication dispensers and Amazon Alexa are examples of such intelligent personal assistants.

On the basis of the applicability

According to the Telecom Regulatory Authority of India, networked medical devices can also be categorized as follows-

Consumer products for health monitoring**-** Fitbit, Nike FuelBand, Withings etc. are examples of devices in this category. These are mainly used for general monitoring of body health parameter. The most common communication medium is BlueTooth to transfer data to a nearby mobile device.

Internally embedded medical devices **-** Implantable cardiac pacemakers, cardiac defibrillators (ICDs), insulin pumps etc. are examples of devices in this category. These devices are implanted inside the patient’s body and communicate wirelessly. Radio frequency technology is used for transmitting data to a remote/bedside monitor. Pairing between the devices is done using the device serial number and/or device model number.

Wearable, external medical devices **-** This category includes portable insulin pumps which often use proprietary wireless protocols to communicate. These devices are attached externally to the body. Data collection and its transmission it to a display device is done thereafter.

Stationary medical devices **-** Devices like chemotherapy dispensing stations that are used for delivering accurate doses of complicated chemotherapy fall into this category. Another example is homecare cardio monitoring for bed ridden patients which is used for tracking their cardiological statistics. (India. Telecom Authority of India, 2015)

Attacks on Internet of Medical Things

IoT based medical systems have constantly been under attacks which include node crash, physical disruption, message alteration, false node, passive information collection, routine attacks, monitoring and eaves dropping, traffic analysis, Denial of Service, node malfunctioning etc. The intention behind these attacks can be to either steal the data, disrupt the system or even damaging the patient’s health fatally. (Tianhe et al., 2015) The physiological data of patients is more vulnerable to attacks like man-in-the-middle attack, falsifying etc. when it is in the transmission stage. In (Devendran et al., 2015), a model is designed to make the security services capable to mitigate unforeseen or unpredictable issues based on experience and knowledge. It consists of inter-service collaboration of Protection, Detection and Reaction services. The paper also talks about IoT healthcare policies of countries like India, Australia, Japan, France, Sweden, Germany, Korea, China, US, EU and the World Health Organization (WHO). However, this coverage on national policies are not in detail. An overview of IoT challenges faced by rural healthcare establishments is presented in (Islam et al., 2015)**.** The IoT technologies being used are cloud computing, grid computing, Big data, Networking, Artificial Intelligence, Augmented Reality, Smart Wearables. In (Zubair et al., 2019) cyber-attacks during the data transmission stage are studied keeping the Bluetooth communication in focus. It is the most widely used communication technology because it is relatively cheaper, can be conveniently used in compact devices and allows ad hoc connection which is suitable for the resource limitation of IoT based healthcare systems. Attacks on such systems are often launched by exploiting Bluetooth communication vulnerabilities. Blue Smacking, Blue Snarfing, Bluejacking, Blue Bugging, Blue Printing, Mac Spoofing, Man in the middle/ Impersonation are some of the attacks carried out to exploit the vulnerabilities of Bluetooth based systems**.** (Cansu and Hamm, 2016) mentions some security controls that the healthcare industry must adopt in order to mitigate security risks to IoT based systems. Strong access control mechanisms ensure that the data is available only to the authenticated users and any kind of unauthorized access to the vital health data of the patients is restricted. Employee awareness about the information security protocols and countermeasures. Firewalls, IPS, IDS, ingress/egress filtering structures, Internet Protocol Security (IPSec), SSL/TLS, HTTPS should be used. Physical security of IoT healthcare systems is as important as the software tools based logical security for protection against environmental threats, sabotage, theft etc. In (Rehman et. al., 2016) a cloud-based architecture of the IoT ecosystem is presented and the related security threats are analyzed. IoT Sensor nodes are attached to the cloud via a base station. Unprotected web interface, insufficient transfer encryption, weak or no authentication/authorization, insecure network services, privacy issues, insecure cloud and mobile interface, and improper security configurability according to the OWASP Top 10 Project are IoT related issues. IoT Security Framework is developed by dividing the IoT system into 4 layers – Things, Communication, Infrastructure and Data Analytics layer, identifying security requirements at each layer, and providing tight security mechanisms at each layer accordingly.

Application of IoT in healthcare

IoT based applications to fight against COVID – 19

The current pandemic situation due to the COVID 19 or the novel coronavirus has led to massive disruption of the global healthcare, economic and social order. IoT based applications are particularly effective in this situation as it enables efficient monitoring of high-risk patients during quarantine and helps in minimizing human to human contact. Biometric information such as blood pressure, heartbeat, glucose level etc. are carried out using this technology. Some of the direct benefits are reduced errors, lower cost, effective control, enhanced diagnosis and superior treatment. (Ravi et al., 2020) Tracking down the patient zero is one of the critical steps to contain the mass spread of virus borne diseases as it gives a record of all those who have been infected. Epidemiologists all over the world are searching for patient zero in various regions in which using Geographic Information System (GIS) with IoT mobile information is highly helpful. (Emanuele et al., 2019) Hospitals are now using connected thermometers for screening the patients and staff. California based health startup VivaLNK’s has developed a connected thermometer. It provides constant monitoring of any changes in the body temperature in real. Cassia is providing an IoT Access Controller which is used to collect the sensor data and wirelessly transfer to the doctor. The gateway can pair and connect simultaneously upto 40 Bluetooth Low Energy devices while providing a long-range connectivity. This solution is being used at the Shanghai Public Health Center and seven other hospitals in China. Electronic tracker wristbands are being used in Hong Kong to alert authorities when the compulsory home quarantine is not followed by those who have a recent international travel history. (Choudhary, 2020)

Diabetes Treatment and Monitoring

Devices like smart insulin pens, caps, attachments and virtual platforms can help in overcoming problems such as poor insulin adherence, incorrect insulin initiation and titration, and medication errors. Smart insulin pens (Sangave et al., 2017) A functional, closed-loop ‘artificial pancreas’ with implantable and bionic functionalities is also a product of IoT. Smart insulin pumps have now been developed which can even precisely mimic physiological demands.

Personal Continuous Glucose Monitor (CGM) is a device that collects and shows the level of blood glucose continuously in real time. (Mcadams and Rizvi, 2016) The devices like Ambulatory Blood Pressure Monitoring System (AMBP), Hypoglycemia Detection Alarm, Glucometer, Activity Tracking Wearable Technologies (ATWT), Diet and Nutrition Apps and Target Heart Rate Monitoring Devices (TMD) use advanced sensors and actuators. (Mishra and Naik, 2017)

Implantable cardiac devices

Implantable electrical systems are capable of performing telemetry (sensing) function, in which biological data are collected. Tele-actuation (stimulation) function can also be performed, sometimes in combination with telemetry in a form of closed loop control. Such systems are generally comprised of an internal module which is embedded within the patient’s body, and an external device for transferring the information. (Bazaka and Jacob, 2012)

Pacemaker is a device that is implanted near the heart to send small electrical impulses to maintain the pace of the heart. It is connected to an external programmed monitor which is used to send the impulses and changing the settings. The information can be accessed over the Internet after authentication and authorization. Unsecured communication between the programmed device and pacemaker creates scope for cyber-attacks. (Kulkarni and Vijaykumar, 2016)

IoT enabled Asthma Management

Medications like glucocorticoids, anticholinergics and beta antagonists are required to be inhaled by the asthma patients. Smart inhalers are small devices used for the purpose of delivering such medications and self-monitoring. IoT based inhalers are basically sensors that are added as a clip on existing inhalers. A GPS module tracks when and where a patient has taken puffs. Inhaler usage is conversed to a mobile application using Bluetooth. Some devices are even able to detect the air-quality in real-time, sending alerts to the users. The collected data can be shared with doctor as well to enable remote-monitoring and ensuring medication adherence. A study conducted by Allied Market Research says that the worldwide smart inhalers market size stood at $34 million in 2018 and a further increase during the forecast period is expected to be at $1,406 million by 2026, with a CAGR of 58.4% from 2019 to 2026. (Kunsel and Pandey, 2019)

IoT for Hospital Management

IoT-driven non-invasive monitoring solutions are used for hospitalized patients who require close medical attention. Sensors collect comprehensive physiological data which is stored and analyzed on cloud. The processed data can then be sent wirelessly to the healthcare providers for further analysis and action. Masimo Radical 7 is one such system that provides bedside monitoring and transport devices for patients. This device can wirelessly send data for live display. (Niewolny, 2020) IoT is also being used in the hospitals for purposes other than patient care. There are systems for tracking the real time location of medical equipment such as oxygen pumps, wheelchairs, defibrillators, nebulizers etc. Prevention of infection spread is one of the major challenges for the healthcare providers. IoT enabled devices for monitoring hygiene are available that help in avoiding patients from getting infected. IoT sensors are also being used for asset management at hospitals. Pharmacy inventory control and environmental monitoring like keeping a check on the refrigerator temperature, humidity and temperature control is one of the many use cases. (Karjagi and Jindal, n.d.)

IoT based healthcare wearables

Any device which can be attached to the human body as utility gadget or clothes is termed as a healthcare wearable. Such devices are capable of collecting and communicating health related data to the medical specialists, remote servers, artificial intelligence (AI) based agents and emergency contacts. Fitness trackers and smart watches are the most popular examples of healthcare wearables. One interesting application in this field is Kardia from AlivCor which can serve as an alternative to electrocardiogram (ECG) test. This wearable can monitor the circadian rhythm of heart in thirty seconds to detect any signs of atrial fibrillation. IoT enabled wearables are also being used to better the lives of physically challenged people. (Albesher, 2019) Smart bracelets and rings with an AI platform by CloudMinds is used in China to provide continuous monitoring of vital signs of coronavirus like temperature, heart beat and blood oxygen levels. (Choudhary, 2020)

Challenges in implementation of IoT in healthcare

Data security and privacy

With the increasing trend of medical systems going digital, the distribution of patient information with not only doctors but with authorized employees, agents, contractors, health insurer etc. has become necessary. As the medical equipment get connected to the web-enabled IT systems, they become prone to cyber-attacks from threat agents like malicious hackers, computer virus, malwares etc. The general motive behind carrying out such attacks is to gain access to critical information related to the patients. Such information like the patient's full name, social security number, driving license number, bank account number, passport details, home address etc. are categorized as Personal Identifiable Information (PII). The Electronic Health Record (EHR) of a patient contains data like the credit card number, address, employer and insurance information. Attackers can use this information to open a new credit card in the victim's name, take bank loan or even get high priced narcotics from medical insurer of the victim. Hence, maintaining the data privacy and security of IoT based healthcare systems is of utmost importance.

Interoperability: Integrating multiple devices and platforms

Interoperability can be defined as the degree to which diverse devices, systems, platforms and departments can be integrated. The Internet of Things is built upon a number of different communication protocols like Internet Protocol version 6 (IPv6), Low Power Wireless Personal Area Network (6LoWPAN), ZigBee, Bluetooth Low Energy (BLE), Z-Wave, DASH7, Near Field Communication (NFC) etc. (Al-Sarawi, 2017) There has not been a consensus reached by the IoT device manufacturers regarding common communication protocol and standards. Therefore, IoT enabled systems are generally composed of heterogenous devices operating upon different platforms and data communication standards. Data aggregation becomes difficult because manufacturers end up creating their own ecosystem of IoT devices which do not work with applications from other manufacturers.

Information Security Challenges

IoT based healthcare systems are vulnerable to cyber-attacks as the Internet connectivity increases attack surface. The entry points for the attackers increase as the number of IoT devices in the network increases. Authentication and authorization mechanisms are used for controlling access to such systems; however, attackers often find ways to gain unauthorized access by launching attacks which are discussed in the next section. Encryption of critical patient related data is done using cryptosystems which use algorithms like Rivest-Shamir-Adleman (RSA), Triple Data Encryption Standard (DES), Blowfish, Twofish, Advanced Encryption Standard (AES) etc. However, it is challenging to implement such cryptosystems in IoT devices because of low power and low computational ability.

Apart from implementing logical software-based security controls, physical security of IoT devices is also critical. Sensors, actuators and other components can be stolen, tempered with or damaged which can lead to even death of the patient. Smart healthcare systems can even be used to listen to communications. For this purpose, stolen IoT devices can be reprogrammed and redeployed in the original position without the knowledge of the owner. (Sun et al., 2019)

Healthcare devices are at a higher risk due to the IoT related vulnerabilities because these can be exploited to even fatally damage a person. Former Vice-President of USA Dick Cheney revealed in an interview with '60 Minutes' that he had his doctors disable the wireless capabilities of his Pacemaker to prevent a possible assassination attempt. (Chacko and Hayajneh, 2018) In 2016, Johnson and Johnson had made an announcement informing the users of their One Touch Ping insulin pump about a security vulnerability that could be exploited by attackers to manipulate the insulin dose of diabetic patients. According to a report on protected health information data breach, about 57.5% of threat actors are the internal employees of healthcare organizations. (Widup et al., 2018) Since internal actors have access to the systems that store patient's information, instances of privilege abuse are common. Such a breach of information security, i.e., unauthorized access to databases are difficult to detect.

One more challenge faced by the healthcare sector is that the security patches and updates are not installed on time. Healthcare professionals rely on the smart clinical devices to treat patient round the clock. The downtime required for the testing and installation of software patches is often not affordable for doctors keeping the patient care on priority. Outdated systems are a major loophole that the attackers take advantage of, to gain access to the network. (Sherri, 2019)

It is observed that generally healthcare organizations do not have network segmentation for separating IoT devices from the rest of the network. Network segmentation is an architectural approach by which an organization's network is further divided into smaller segments or subnets. This is done to enable the network administrators to control the traffic flow between subnets according to the granular policies. (PaloAlto Networks, n.d.) This is a threatening problem because security features generally do not come embedded from the manufacturer, rather they need to be installed as an add-on feature. With a common network for all the devices, it is not possible to configure the IoT devices network with special security controls. This enhances the chances of human error or negligence like system configuration errors, discrepancy in audit logs, unauthorized access control or lack of processes governing the device use. (Anastasios, 2019)

According to a report by Vectra, Hidden DNS and HTTPS Tunnels are the most exploited methods by the attackers to breach the network security. (Vectra Industry Research Report, 2020) DNS tunnels are used to insert commands and move stolen data by the attackers to communicate secretly with a computer. This method can also be used to insert malwares in the remote systems.

Attacks on IoT based healthcare systems

This section describes some common cyber-attacks on healthcare systems and their impact.

Denial of Service (DoS) Attack

A DoS attack on a system prevents the legitimate users from accessing it. Attackers overload the resources of the target computer by flooding it with non-legitimate service requests or traffic. This attack on healthcare systems can prove to be fatal for patients who rely on medical devices for their drug dosages and other critical functions. Distributed Denial of Service (DDoS) attack is a type of DoS where multiple victim computers are used as bots to carry out the attack on a single system. This group of bots or the 'botnet' is a network of inter-connected computers controlled remotely by the attackers, also called bot-herders. Bots are created by exploiting vulnerabilities like open unprotected network ports or via trojans or other malwares. Once compromised, these computers receive commands from the attackers via Internet Relay Chat (IRC) or other tools. Since this network of bot computers is distributed over the Internet, it becomes difficult to track the controllers.

Healthcare systems are favorite targets of cyber-attackers because of the highly critical and valuable data and the most vulnerable systems that store it. It is easier to attack these systems because of the unpatched software vulnerabilities in the outdated computer and other devices. Healthcare organizations do not give much attention to the security aspects of IoT devices as upgrading a system requires downtime which is generally avoided. There is no regulation for the IoT device manufacturers to include security mechanisms in the devices. Cheap IoT devices are readily available that generally do not have enough security measures.

Ransomware Attack

It is a kind of malware which leaves the files in the victim computer in an encrypted state. The attacker then demands a ransom for restoring the data. A message is displayed on the system about the payment instructions. Victims are made to pay heavy amounts in Bitcoin in exchange for the decryption key. The common method for these malwares to reach the target system is through phishing campaigns. Attackers send a seemingly legitimate email persuading the receiver to click on a link. This link when opened, downloads and installs the malware into the host computer.

A ransomware named WannaCry first appeared on May 12, 2017 and infected over 300,000 systems worldwide. One of the notable victims is the British National Health Service (NHS). Hospitals in Britain were forced to divert their patients as the doctors were not able to access their medical records. As per a report by Internet of Things firm Armis, WannaCry ransomware is still active on over 145,000 devices globally. (Ben, 2019) It is considered as the most widespread and destructive cyber-attack in the history of IT world. WannaCry spreads through its worm element, which has the capability to spread to other computers across the network. The associated vulnerability with this ransomware was in the Microsoft SMB Protocol, which is used in Windows OS based systems for file transferring. This exploit is called EternalBlue for which Microsoft had already released a security patch before WannaCry hit the world. Systems which were not updated on time got attacked. (Mackenzie, 2019) According to a report by Fortune, healthcare providers and medical facilities have experienced a spike in ransomware attacks after the onset of the COVID – 19 Pandemic. (Gallagher and Bloomberg, 2020) Attackers are targeting clinical labs and major hospitals involved in vaccine development and testing, taking advantage of the global health emergency. This not only prevents the medical staff from accessing health data of patients, drug dosage history and other critical information, but also puts patient's privacy at risk. Many a times, attackers threaten to publicize the data. This variation is also called as leakware or doxware.

Medjacking

This attack vector was first researched by the TrapX labs in 2015. Medjack or "Medical Device Hijack" is the term given to an attack where the hacker creates a backdoor by hijacking a medical device to gain entry access into the system. Once it is created, the backdoor is used to exfiltrate patient data from across the healthcare network, install malwares, manipulate the configurations or even completely shutting down the systems. Researchers at TrapX found that in three separate hospitals, a variety of medical devices were severely compromised. These devices included X-Ray equipment, Picture Archive and Communication System (PACS) and Blood Gas Analyzers (BGAs). In their report, an unnamed hospital was under attack through three BGAs which were hijacked. The attackers had enabled backdoors through the BGAs into the organization and were moving laterally across the network to steal hospital data. It was also discovered that two malwares namely Zeus and Citadel were stealing passwords within the hospital. Diagnostic equipment like PET scanners, CT scanners, MRI machines etc. are also easy targets for such attacks. (TrapX Labs, 2017)

Technical Vulnerabilities

There have been rapid advances in the Internet of Things when it comes to the healthcare sector. However, information security of these devices has got less attention. Inadequate security measures have led to a number of vulnerabilities in such systems which serve as an easy medium for the attacker to materialize their malicious intents.

In U.S., the Food and Drug Administration (FDA), issued a warning in March, 2020 about a set of cybersecurity vulnerabilities referred to as 'SweynTooth'. (U.S. Food and Drug Administration, 2020) The wireless communication technology Bluetooth Low Energy (BLE) is the main target of these vulnerabilities. The researchers who discovered these vulnerabilities have classified them on the basis of their types and behavior on the affected BLE devices –

Crash **–** These vulnerabilities can crash a device remotely through triggering of hard faults. Some incorrect code behavior or memory corruption can cause this situation.

Deadlock **–** These vulnerabilities impact the availability of a BLE connection. Generally, the users need to power off their device and then power on to re-establish the connection, which essentially is a kind of Denial-of-Service.

Security Bypass **–** It allows the attackers in radio range to bypass the latest security pairing mode of BLE. This means that the attacker can easily gain read and write access to the device's functions, which otherwise are supposed to be accessed only by authenticated users. (Matheus et al., n.d.)

Recently, a series of zero-day vulnerabilities called as Ripple20, has been discovered by JSOF research lab. (Kol and Oberman, 2020) There are 19 vulnerabilities in this series found in the 'Treck TCP/IP' stack which is commonly used in the IoT devices. The impact of these vulnerabilities if exploited, include remote execution of the device code and information leakage both of which can prove to be even life threatening. Remote Code Execution (RCE) means that an attacker can take over the control of the device even from the outside of the network. Once the devices within a network are compromised, further attacks can simultaneously be broadcasted to them and more damage can be caused on a large scale.

One more problem with IoT based medical devices is that the increased attack su1rface. This is because of their special structures and requirements. The attack surfaces can be distinguished into three layers based on the underlying vulnerability and device composition. (Miao et al., 2020)

Protocol Interface Layer – On this attack surface, lie the vulnerabilities like weak authentication, leaky transmission of sensitive information, unsafe remote management interface etc.

Software Layer – Incorrect configuration strategy, unsafe application service, leakage of sensitive information in the firmware, unsafe operating system, unsafe bootloader etc. are the vulnerabilities categorized in this layer of the attack surface.

Hardware Layer – The vulnerabilities on this layer of attack surface include leakage of sensitive information through the hardware, unprotected flash chip, unsafe debugging interface etc.

The IoT device manufacturers generally leave the debug interface like an UART on the circuit board which is used for repairing purposes later. A weak or no authentication mechanism may give the attackers a chance to obtain high authority shell to manipulate or change the firmware. Flash chips are used for non-volatile storage of firmware. If read-write access is not properly restricted, attackers can easily read the firmware for analysis or can even write it and bypass the authentication of interface access. Because of light-weight storage solutions in IoT devices, security mechanisms are generally not implemented by the developers. Hence, leakage of critical information through the firmware is an easy way for attackers to steal the data. Incorrect configuration strategy by the network security managers is also a major reason of security failures of even high-end medical systems. For example, in 2019, Benjamin Kunz in his research discovered zero-day vulnerability in the Telestar Digital GmbH IoT Radio devices that enabled attackers to remotely hijack the device without even any user interaction. The researchers exploited the weak authentication policies and were able to brute-force the device in 10 minutes. (Paganini, 2019)

Existing Regulations and Standards for the Healthcare Sector

Health Insurance Portability and Accountability Act (HIPAA)

Implemented in 1996 in USA, this act aims to protect the privacy and security of health information of the citizens. It regulated the flow of healthcare information, set up guidelines as to how personally identifiable information of a patient can be maintained by the healthcare and healthcare insurance industries and protected from fraud and theft, and addressed limitations on healthcare insurance coverage. The law mandates that the healthcare organization responsible for data collection, storage and processing must notify the impacted patients in the event of a security breach within 60 days of the incident. There are five rules namely the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, Omnibus Rule and the HIPAA Enforcement Rule. The entities covered under HIPAA are required to implement the safeguard measures to protect the confidentiality, integrity and availability of Protected Health Information (PHI). (U.S. Department of Health & Human Services, 2019)

U.S. Food and Drug Administration (FDA)

This U.S. agency allows medical devices as long as there is assurance that the risks are outweighed by the benefits to patients. (U.S. Food and Drug Administration, 2020) According to the guidelines released by the agency, Medical Device Manufacturers (MDMs) are responsible for remaining vigilant about the cybersecurity risks related to their devices. It is the responsibility of the Healthcare Delivery Organizations (HDOs) for the evaluation of network security of their hospital systems. Both these entities are responsible for mitigating the patient safety risks and ensuring proper device performance.

EU's General Data Protection Regulation (GDPR)

The regulation came into force on May 25, 2018 and is applicable for all those who collect, process or store personal data of the data subjects, i.e., people residing in the EU. Many aspects of this law are applicable for the healthcare industry as medical devices collect huge amount of patient information that are generally high 'risk'. According to GDPR, health related data falls under its 'Special Category' and hence, it is mandatory to first seek consent from the data subject before data collection. Also, the law makes it compulsory that a Data Protection Impact Assessment (DPIA) be conducted when such data are processed. Like HIPAA, the GDPR also requires that the healthcare organizations implement appropriate technical and organizational controls to ensure the confidentiality, integrity and availability of collected data. As per GDPR, patients have the right to access their personal data and related information like the purpose of data collection, type of data collected and processed, with whom the data will be shared and the time period for which the data will be stored. In the event of a data breach, it is mandatory that the concerned organization notifies the affected patients of the incident withing 72 hours of discovery of the data breach.

Digital Information Security in Healthcare Act (DISHA)

Proposed in 2017 by the Ministry of Health and Family Welfare, Govt. of India, this law aims at standardizing the process of collection, storage, sharing and usage of digital health data. It will help in maintain the privacy, confidentiality and security of health-related data. Article 38 and 39 provide the detailed information about the data breach, notification of the breach and associated penalties. Along the similar lines of HIPAA and GDPR, DISHA also entitles the owner of digital health data with certain rights like the power to allow or refuse collection, storage, sharing of their data. The owner has the right to access their data at any point of time and can even get the data corrected in case of any inaccuracy. The data owner must be notified whenever any clinical establishment accesses this data. The data owner is also entitled for compensation if data breach causes any kind of damage to them

Personal Data Protection Bill (PDPB), 2019

Proposed by the Ministry of Electronics and Information Technology in 2019, this bill aims to protect the personal data of individuals and establish a Data Protection Authority of India for controlling the concerned matters. Health data falls under the category of 'Sensitive Personal Data' and through this bill, patients will gain more control over their data as to what data is being collected and how the information is used and shared. In case non-compliance, organizations are liable to pay huge penalties, the maximum fine being Rs. 15 crore or 4% of its total worldwide turnover, whichever is higher.

Proposed solutions to mitigate information security risks

Achieving 100% guaranteed information security and eliminating all the possible risks is not possible however, with the implementation of security best practices and awareness, the impact of threats can be minimized. Following are some of the measures that can be adopted for safe-guarding critical data of patients by the healthcare organizations.

Network Segmentation

It is observed that healthcare organizations do not implement network segmentation and communication of IoT based medical devices happens over the same general network. This is a major vulnerability as discussed earlier. Once an attacker gets through the security layer of Firewall and Intrusion Detection System (IDS), it is easy to attack the devices directly due to a flat network architecture. Network segmentation allows to limit the flow of traffic, type, source, destination and other aspects in small parts of the network. Segmentation of a network can be done either physically or logically. In physical network segmentation, each segment has its separate internet connection, physical wiring and firewall. (Metivier, 2017)

Improved incident reporting mechanisms

It is often noted that an information security breach takes a devastating form just because it was not reported on-time initially. For example, in case of a phishing attack, if the incident is reported as soon as the first person gets attacked, other concerned personnel can be alerted of the possible attack and the damage can be contained. An incident reporting and response team must be formed with clear roles and responsibilities to expedite the process of detecting a breach and controlling its impact.

Information Asset Classification

An efficient information asset classification setup helps the organization in prioritizing the security controls based on the level of sensitivity and impact of the threat. The information collected through the medical devices must be classified in categories like public, internal, classified or restricted. Such classification not only helps the organization in improved risk assessment, but is also crucial for get compliant with information security standards like ISO 27001.

Patching/ Upgrading on-time

History of major cyberattacks on healthcare systems like the WannaCry ransomware or the Mirai botnet attack have revealed a common vulnerability of outdated systems being used in the healthcare organizations. The information security policy of such institutes which deal with sensitive health data of patients must include regular and mandatory upgrades of systems. The current infrastructure must be enhanced so that necessary backups may be taken as and when required during these upgrades.

Risk Assessment and Audit

Healthcare organizations must consider information security as a major module of their company policy. A well-documented procedure must be laid out for carrying out risk assessment. Assets must be identified and their associated threats and vulnerabilities. Risk is the combination of likelihood of a threat to be realized and the impact it may cause to the asset. An efficient risk assessment is instrumental in making a risk mitigation plan. Security audits, internal or external, must also be conducted at least on an annual basis to check if the risk mitigation plan is implemented or not.

IoT Manufacturer's Responsibility

Currently, the manufacturers of IoT based medical devices are not bound by any law to embed security features in the devices. Hence, cheap devices are widely available in the market which are used for medical care purposes with little or no security features. Strict laws should be implemented to make it mandatory for the device manufacturers to adhere to standards and guidelines. Penalties should be levied in case of non-compliance.

Healthcare Provider's Responsibility

In hospitals where IoT based systems are used for patient care, a full-time dedicated IT Team or outsourced IT services from a third-party should be employed for constant monitoring of the organizational network. The security of network architecture must be assessed and reported regularly. Access management system must be efficient enough to restrict data access only to authorized personnel. Patients must be made aware of the personal data collection and type of processing. Data collections should be done after taking consent from the data subject, i.e., patients. When new IoT systems are procured, it is the responsibility of the hospital to ensure that it conforms to at least minimum adequate security standards. The systems must be updated with latest security patches.

User's Responsibility

It is the responsibility of end users to protect the secured login credentials. Users must be well trained with best practices of security, must be aware of the impact should there be any data breach. The passwords must be strong enough and not be shared with anyone. In case of personal medical devices like Fitbit, users must keep the software and device updated with latest security patch releases.

Conclusion

Confidentiality, Integrity and Availability are major pillars of information security and must be ensured for patients using IoT based medical devices. Huge amount of sensitive health related data is collected, processed and stored by these devices. The security aspects of such systems, if overlooked, may lead to unauthorized disclosure and misuse of the data. Attackers generally target healthcare organizations due to lack of security measures generally adopted. Health related data can also be easily sold in black market to gain huge profits. Thus, it is high time that healthcare organizations take strict measures in securing the patient data. Security measures need to be adopted on technical, administration and management level. User awareness is also one of the major keys of information security. Compliance to the industry and government standards and laws must be adhered to. Though India currently does not have any information security law for healthcare in practice, but the proposed drafts of Personal Data Protection and Digital Information Security for Healthcare Act are a significant step towards data privacy issues in the country. A law specifically for regulating the IoT based devices in the healthcare sector should also be introduced

Acknowledgement

The authors wish to acknowledge Symbiosis Centre for Information Technology for providing the library facilities.

Conflict of Interest: There is no conflict of interest among the authors

Funding: Self-funded

Ethical approval: Not applicabl

References

1. Anatomy of an attack MEDJACK. (2017). TrapX Labs - A Division of TrapX Security, Inc. Retrieved June, 2020, from https://trapx.com/wp-content/uploads/2017/08/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf

2. Arampatzis, A. (2019, June 21). Cyber Security Challenges in Healthcare IoT Devices. Retrieved May 20, 2020, from https://www.tripwire.com/state-of-security/security-data-protection/iot/cyber-security-healthcare-iot/

3. Bazaka, K., and Jacob, M. (2012). Implantable Devices: Issues and Challenges. Electronics, 2(4), 1-34. doi:10.3390/electronics2010001

4. Butt, S. A., Diaz-Martinez, J. L., Jamal, T., Ali, A., De-La-Hoz-Franco, E., and Shoaib, M. (2019). IoT Smart Health Security Threats. 2019 19th International Conference on Computational Science and Its Applications (ICCSA). doi:10.1109/iccsa.2019.000-8

5. Center for Devices and Radiological Health. (2020, March). Cybersecurity. Retrieved August 21, 2020, from https://www.fda.gov/medical-devices/digital-health/cybersecurity

6. Chacko, A., and Hayajneh, T. (2018). Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 0(0), 155079. doi:10.4108/eai.13-7-2018.155079

7. Choudhary, M. (2020, May 01). How IoT can help fight COVID-19 battle. Retrieved August 25, 2020, from https://www.geospatialworld.net/blogs/how-iot-can-help-fight-covid-19-battle/

8. Davidoff, S. (2019). Data Breaches: Crisis and Opportunity [Electronic]. United States: Addison-Wesley Professional.

9. Eken, C., and Eken, H. (2018). Security Threats and Recommendation in IoT Healthcare. Proceedings of the 9th EUROSIM Congress on Modelling and Simulation, EUROSIM 2016, The 57th SIMS Conference on Simulation and Modelling SIMS 2016. doi:10.3384/ecp17142369

10. Gallagher, R., and Bloomberg. (2020, April 01). Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus. Retrieved May 01, 2020, from https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/

11. Garbelini, M. E., Chattopadhyay, S., and Wang, C. (2020, July 14). Unleashing Mayhem over Bluetooth Low Energy. Retrieved August 15, 2020, from https://asset-group.github.io/disclosures/sweyntooth/

12. Gong, T., Huang, H., Li, P., Zhang, K., and Jiang, H. (2015). A Medical Healthcare System for Privacy Protection Based on IoT. 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP). doi:10.1109/paap.2015.48

13. India. Telecom Regulatory Authority of India. (2015, July 23). Internet of Things. Retrieved May 20, 2020, from https://trai.gov.in/sites/default/files/TD_24082015.pdf

14. IoT in Healthcare Market Worth $534.3 Billion By 2025: CAGR: 19.9%. (2019, March). Retrieved August 24, 2020, from https://www.grandviewresearch.com/press-release/global-iot-in-healthcare-market

15. Karjagi, R., Dr., and Jindal, M. (n.d.). IoT in Healthcare Industry: IoT Applications in Healthcare. Retrieved July 7, 2020, from https://www.wipro.com/en-IN/business-process/what-can-iot-do-for-healthcare-/

16. Kunsel, T., and Pandey, D. (2019, June). Smart Inhalers Market by Product (Inhalers and Nebulizers), Indication (Asthma and COPD), and Distribution Channel (Hospital Pharmacies, Retail Pharmacies, and Online Pharmacies): Global Opportunity Analysis and Industry Forecast, 2019 - 2026. Retrieved from https://www.alliedmarketresearch.com/smart-inhalers-market

17. Massaro, E., Kondor, D., and Ratti, C. (2019). Assessing the interplay between human mobility and mosquito borne diseases in urban environments. Scientific Reports, 9(1). doi:10.1038/s41598-019-53127-z

18. Mcadams, B., and Rizvi, A. (2016). An Overview of Insulin Pumps and Glucose Sensors for the Generalist. Journal of Clinical Medicine, 5(1), 5. doi:10.3390/jcm5010005

19. Metivier, B. (2017, June 16). Network Segmentation: Considerations for Design. Retrieved August 20, 2020, from https://www.tylercybersecurity.com/blog/network-segmentation-considerations-for-design

20. Paganini, P. (2019, September 10). Million of Telestar Digital GmbH IoT radio devices can be remotely hacked. Retrieved April 12, 2020, from https://securityaffairs.co/wordpress/91069/hacking/telestar-iot-radio-devices-hack.html

21. Rahman, A. F., Daud, M., and Mohamad, M. Z. (2016). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. Proceedings of the International Conference on Internet of Things and Cloud Computing - ICC '16. doi:10.1145/2896387.2906198

22. Sangave, N. A., Aungst, T. D., and Patel, D. K. (2019). Smart Connected Insulin Pens, Caps, and Attachments: A Review of the Future of Diabetes Technology. Diabetes Spectrum, 32(4), 378-384. doi:10.2337/ds18-0069

23. Seri, B. (2020, March 27). Two Years In and WannaCry is Still Unmanageable. Retrieved July 25, 2020, from https://www.armis.com/resources/iot-security-blog/wannacry/

24. Singh, R. P., Javaid, M., Haleem, A., and Suman, R. (2020). Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes and Metabolic Syndrome: Clinical Research and Reviews, 14(4), 521-524. doi:10.1016/j.dsx.2020.04.041

25. Sun, Y., Lo, F. P., and Lo, B. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access, 7, 183339-183355. doi:10.1109/access.2019.2960617

26. U.S. Department of Health & Human Services. (2019, January 04). Health Information Privacy. Retrieved August 18, 2020, from https://www.hhs.gov/hipaa/index.html

27. U.S. Food and Drug Administration. (2020, March 3). FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy. Retrieved June 27, 2020, from https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0

28. Vectra Industry Research Report. (2020). The 2020 Spotlight Report on Healthcare. Retrieved June, 2020, from https://content.vectra.ai/rs/748-MCE-447/images/IndustryResearch_2020_Spotlight_Report_on_Healthcare.pdf

29. What Is Network Segmentation? (n.d.). Retrieved May 25, 2020, from https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

30. Yeole, A. S., and Kalbande, D. R. (2016). Use of Internet of Things (IoT) in Healthcare. Proceedings of the ACM Symposium on Women in Research 2016 - WIR '16. doi:10.1145/2909067.2909079

31. Yu, M., Zhuge, J., Cao, M., Shi, Z., and Jiang, L. (2020). A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices. Future Internet, 12(2), 27. doi:10.3390/fi12020027

32. Zubair, M., Unal, D., Al-Ali, A., and Shikfa, A. (2019). Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices. Proceedings of the 3rd International Conference on Future Networks and Distributed Systems - ICFNDS '19. doi:10.1145/3341325.3342000