الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جامعة وهران 1 أحمد بن بلة
Université Oran 1
كلية العلوم الدقيقة والتطبيقية
Faculté des sciences exactes et appliquées

Module Security System Information

Subject : Search About healthcare IOTs Security

Presented By : Hichem Belguendouz

Juin 10, 2021

Table of Materiel

List of Figures

Abstract :

Computer Science and Electronic engineering have been combined into one of the newest technology, the Internet Of things. IoT Devices are everywhere nowadays, which include the healthcare field. It offers many benefits, including being able to monitor patients more closely and using data for analytics. The importance of IoT devices and data can be dangerous, so implementation of security is very important to save the patient's lives and data.
The IoTs are small computers any Electronic attack can lead to compromise them. What if these hacked devices can kill someone, it is critical and a real scenario can happen at any time. Most Healthcare providers are medical device makers, which may not be familiar with security and attacks. They might be using unpatched systems or unsecured radiofrequency. This paper review pacemaker device vulnerabilities, attacks, and security issues and solutions.

1-What Is IoT?

Figure 1: Intenet of Things

The Internet of Things (IoT) in simple words is a network of physical objects that are embedded with sensors, systems, and other technologies to be connecting and exchanging data with other devices and systems over the internet called machine-to-machine communication (M2M). The IoT is making the Word smarter, dynamic, and responsive to humans Lives.
These devices range from ordinary house Objects to sophisticated industrial tools. With more than 46 billion connected IoT devices today, according to statistics experts are expecting this number to grow to 10 billion by 2020 and 75 billion by 2025.

2-Fields of technology for Internet of Things (IoT)

Here are **five fields of technologi**es we think are the most wide areas to use for IoT patent filings:

2.1 6G and 5G

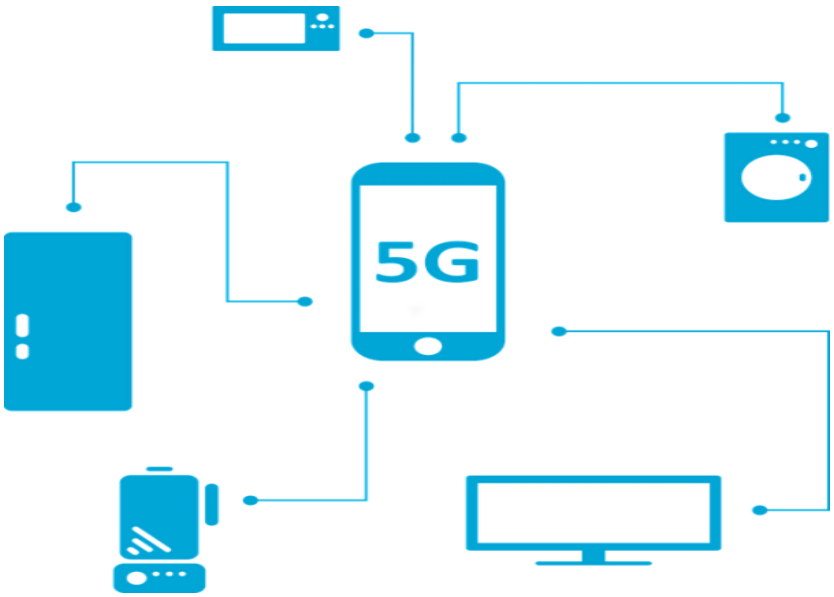

Figure 2: G5 & 6G

6G & 5G is the next steps in the evolution of mobile wireless technology, and it is suggested that these new generations will bring higher speeds, lower latency, & more reliable connectivity to devices. Enabling a host of new applications in the field of IoT. For this reason, many global IT companies are in a patents “arms race” for compiling their own 5G & 6G related patent portfolios.

IPlytics and the Technical University of Berlin complied that Huawei the Chinese manufacturer is on the top of the ranking in statistics in February 2020. IT has more than 3,000 patent applications related to the 5G-standard technology filed and plus than 1,200 of these granted. Second on the list are Chinese provider ZTE, and South Korean manufacturers Samsung and LG. As the patenting process may take several years, the statistic also reflects which companies have filed patents more recently. Finnish company Nokia and Swedish company Ericsson are fifth and sixth on the list sequentially. Lastly, US companies Qualcomm and Intel took seventh and eighth place.

2.2 Electrical Grid Industry

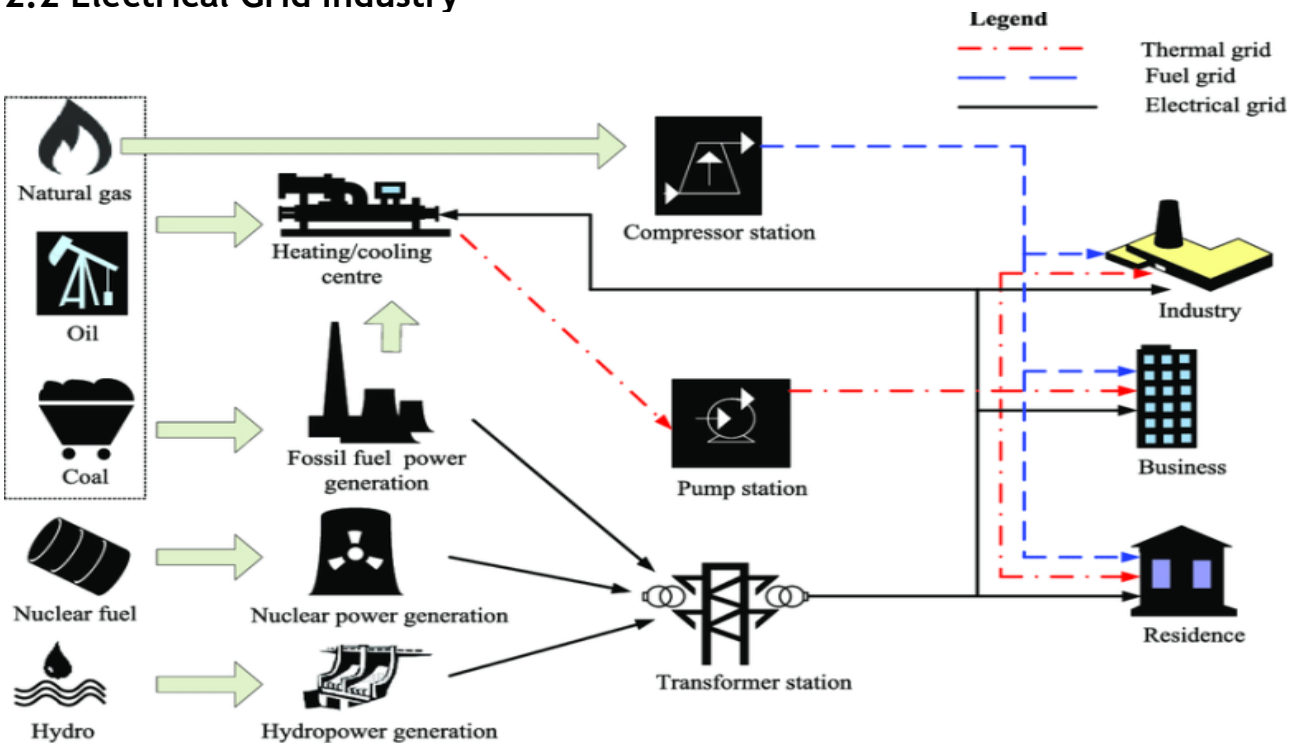

Figure 3: Electrical Grid Industry

An electrical grid is an interconnected system for electricity delivery from producers to users. Electrical grids vary in scope and can cover whole countries or continents. A smart grid serves several objects and the movement from common electric grids to intelligent grids. The idea was driven by multiple factors such as :

a) The deregulation of the energy Industry.
b) Change the degrees of production of electricity.
c) Decentralization (distributed energy).
d) Changing regulations, and more.

Although electrical grids are extensive, as of 2016 1.4 billion people worldwide were not connected to an electricity grid. As electrification increases, the number of people with access to grid electricity is growing. About 840 million people in all the world had no access to grid electricity in 2017, down from 1.2 billion in 2010.

2.3 Autonomous/Driverless Vehicle Technology

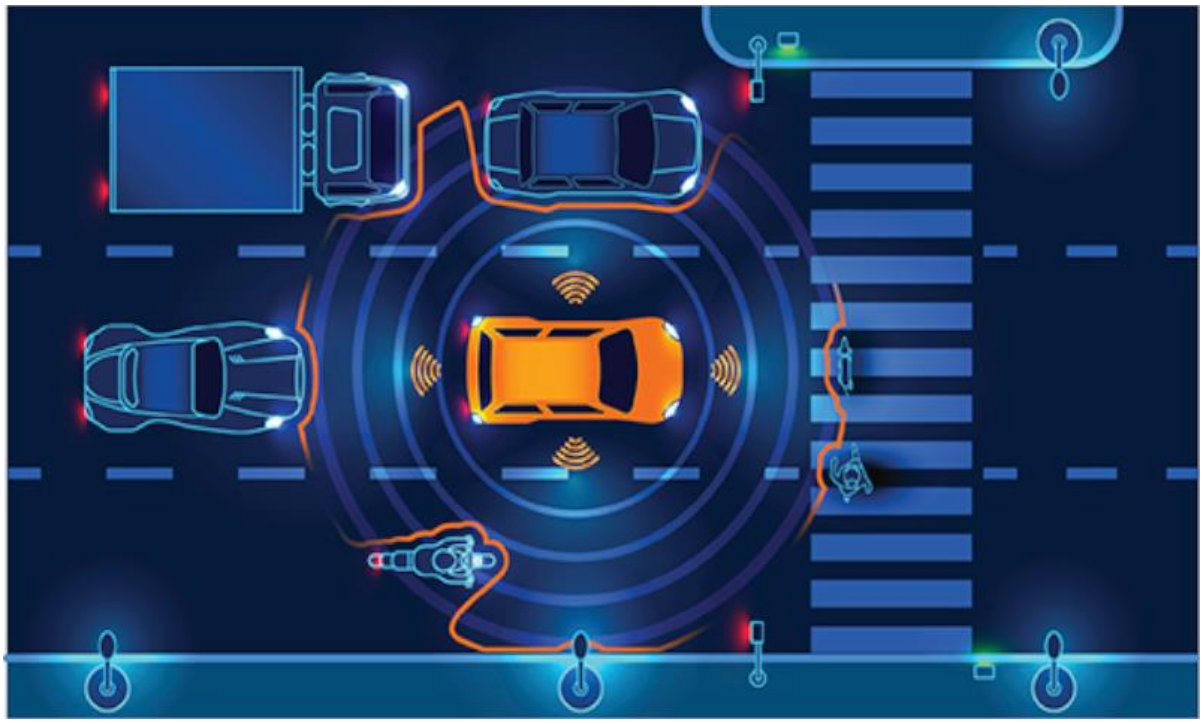

Figure 4: Autonomous/Driverless Vehicle Technology

Autonomous vehicles require an enormous amount of data collecting and processing. Driverless cars require interconnectivity when updating algorithms based on data exchange. For example, driverless cars may exchange information in real-time, such as each vehicle's traveling speed, traffic information or road closures, weather updates, and upcoming obstacles.

All of this data is shared between IoT-connected cars and uploaded wirelessly to a cloud system to be analyzed and used to improve automation. For this reason, this field is closely associated with the roll-out of 5G, which will enable wireless connections with the requisite bandwidths required for such a large information exchange.
in 2018, the EPO reported a sharp increase in European patent applications filed for self-driving vehicles.

2.4 Smart Cities

Figure 5: Smart Cities

The “Smart cities” term refers to the use of IoT devices such as connected sensors, meters, and lights, to collect and analyze data. The cities are using this data to improve service, public utilities, infrastructure, and more. According to a report issued by US attorneys Kilpatrick Townsend & Stockton LLP, “Smart City IoT” has one of the highest numbers of patent filings in the US.

This finding may be due to the wide range of activities (from public safety to traffic regulation to air quality). The deployment of IoT would be beneficial in an urban setting and to the increasing adoption of IoT projects by local authorities. Large multinational companies, such as Honeywell, IBM, Ford, Toyota, and Samsung have all been filing patent applications in this area, especially in the US.

2.5 Healthcare

Figure 6: Healthcare

Patients in hospitals frequently interact with various connected monitors and scanners, equipped with devices that can collect and forward data. A sub-part of the IoTs, known as the "Internet of Medical Things" (or "IoMT"), describes a connected infrastructure of devices, software, hardware, and services used to process and analyze data for decision making by healthcare specialists in a patient's treatment.

In the hospital environment, the IoT is typically about raising patient safety and/or optimizing processes to allow medical practitioners to work together across disciplinary boundaries to carry out and individualize patient care. Some Statistics in 2016 was predicted that by the year 2020, 40% of IoT technology will be health-related and in Five next years years' time (by 2025), the IOMT market may well be worth roughly US$188.2 billion according to Deloitte.

3-What are the main benefits of IoT in healthcare?

The Internet of Things is redefining the healthcare field as we know it. We're moving on to a completely new level when it comes to the way that people, devices, and apps interact when delivering healthcare solutions. IoT has given us a new outlook as new tools that provide an integrated healthcare system. Consequently, the care that is provided is of a higher standard.

The use of IoT in the Medical field allows for the automation of processes that have previously taken time. Certain processes earlier allowed human error. For illustration, nowadays many hospitals use connected machines to control the airflow and temperature in operating theatres.

The benefits of IoT in healthcare are seemingly unlimited such as:

• Decreased the number of Errors: IoT allows for the accurate collection of data, automated workflows, and minimizes wasted time. However, most importantly it decreases the risk of error.

• Decreased costs: Patient monitoring workflow can be done in real-time, Which will reduce the need for doctors going out and making visits To them. Connected home care systems facilities will also help decrease hospital stays.

• Better patient experience: A connected healthcare network creates an environment that meets each patient's needs. This means augmented diagnosis accuracy makes for a better patient experience.

• Advanced disease management: They can continuously monitor patients using real-time data. This means that they can detect any disease before it spreads and becomes dangerous.

The improvements of IoT have the potential to really transform healthcare positively. However, we must be careful. Patient data is very very sensitive and if it's shared inappropriately or misused in some way it has the potential to damage people's privacy. Guaranteeing hospitals have secure and manageable infrastructure is necessary for the healthcare sector.

4-Why is the state of medical IoT so scary?

To ever Simplify Little a little - medical technologies are evolving so quickly. from the digitization of medical record-keeping to the advent of devices that actively help monitor and manage treatment, such as heart-rate monitoring, portable diagnostic devices, insulin pumps, and more

Nonetheless, that evolution might be happening so fast, when you consider the security issue that has been revealed about many of the devices that store our treatment information and even help manage our care. There are a lot of layers to this problem, according to the experts. For one thing, the companies making devices are totally medical device makers, which might not be familiar with security and threats

The Issue that is happening is at the coding level(software), the devices that were created to speed up and mechanize the actual tasks involved with patient care are Totally insecure. Many security experts in the field prove that is possible to hack medical devices such as jay radcliff in 2011 has found a way to hack his insulin pump and they have been trying to warn healthcare providers and the public that medical IoT Gadgets are generally unsafe.

As we know that the medical devices use Computers. otherwise, these Computers can be hacked so nothing is insured to us that Medical IOT are safe in one way or another.

- **Why This Happening:** Part of this issues are:
    1. Patching : a big section of medical IoT devices wasn't designed to be connected to the Internet, So the organization that creates them aren't able to release regular security patches.

    2. HIPAA Compliance: most efforts that are being spent on security in the healthcare field are focused on HIPPA compliance. This Terms Urging that patient information be private, but it means that there's plenty of work being done on issues that aren't medical IoT(we will discuss more HIPAA compliance in the next section).

5-HIPAA Security Rule

a) What is Hippa Compliance

The Health Insurance Portability and Accountability Act (HIPAA), is the standard for digital patient data safeguarding. Companies that deal with protected health Infos (PHI) must have physical, network, and process security measures in order and follow them to ensure HIPAA Compliance. Covered entities (all who providing treatment, payment, and operations in the medical field) and business associates (anyone who has access to patient information and can provide support in treatment, payment, or operations) must meet HIPAA Compliance rules.

b) The Security Rule

The HIPAA Security Rule establishes international standards to secure patient personal health data which is produced and maintained by the related health providers. The Security Rule requires proper administrative, physical & technical protection to ensure the confidentiality, integrity, and security of digital protected health information.

c) THE HIPAA PRIVACY AND HIPAA SECURITY RULES

According to Health and Human Services owned by the US Department, the HIPAA Privacy Rule, or Standards for Privacy of Individually Identifiable Health information creates standards to protect some health information. In addition, the Security Rule creates a national set of security standards for protecting specific health information that is held or transferred in Digital form.

The Security Rule operationalizes the Privacy Rule's protections by processing the technical and non-technical safeguards that related entities must put in place to secure individuals' electronic PHI (e-PHI). Within HHS, the Office for Civil Rights is responsible for effectuating the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

d) What is the Security Risk Assessment Tool (SRA Tool)

The tool is designed to help healthcare providers conduct security risk assessment steps as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service Electronic Health Record (EHR) Incentive Program.

The tool diagrams HIPAA Security Rule safeguards and provides enhanced functionality to document how your organization implements safeguards to mitigate, or plans to mitigate, identified risks.

Some Features of This Tool :

- Enhanced user interface.
- Modular workflow.
- Custom assessment logic.
- Progress tracker.
- Threats & vulnerabilities rating.
- Detailed reports.
- Business associate and asset tracking.
- Overall improvement of the user experience.

6-Understanding The Risk of exploiting Implanted Medical Devices

When vulnerabilities can be a high risk to human lives, So we should take them seriously. In today's Technology Innovation, cybersecurity in healthcare and protecting information is mandatory for the normal functioning of organizations. Many healthcare organizations have various types of specialized hospital information systems such as EHR systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems, and computerized physician order entry systems. Additionally, thousands of devices that comprise the Internet of Things must be protected as well. These include smart elevators, pacemakers, ventilation, and air conditioning (HVAC) systems, insulin pumps, remote patient monitoring devices, and others.

We are going To demonstrate how that can such a vulnerability in the medical device can be fatal. In the next section, We took an example of a pacemaker and how can hackers Billy Rios & Jonathan Butts Find an exploit that can kill a patient.

a) How bad people can hack your heart.

This scenario has not happened yet but there is a TV show called Homeland Dangerous people "terrorist" finds out that the Vice President has a problem in his heart and his pacemaker can be remotely accessed with the correct serial number “we'll demonstrate all the details in the next sections”. The terrorist convinces a congressman to retrieve the serial number in some way, and then his attacker helper uses the serial to remotely access the pacemaker. Once the hacker gets access to the pacemaker, he instructs the implantable device to deliver a lethal jolt of electricity. The vice president falls, grabs his chest from pain, and dies after several seconds.

In 2013, former Vice President Dick Cheney revealed that his doctor ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt. In addition, despite literally being a scenario from Homeland, that is a valid fear.

Let's demonstrate how can a hacker compromise a pacemaker device and can make your life dangerous.

b) How Does pacemaker work

A pacemaker is a small tool implanted in the chest. It sends electrical signals to start or organize a slow heartbeat. Its most often placed in the chest just under the collarbone, as you will see in the picture. A pacemaker device may be used if the heart's natural pacemaker (The sinoatrial node) is not working well causing a slow heart rate or rhythm, or if the electrical pathways are blocked.

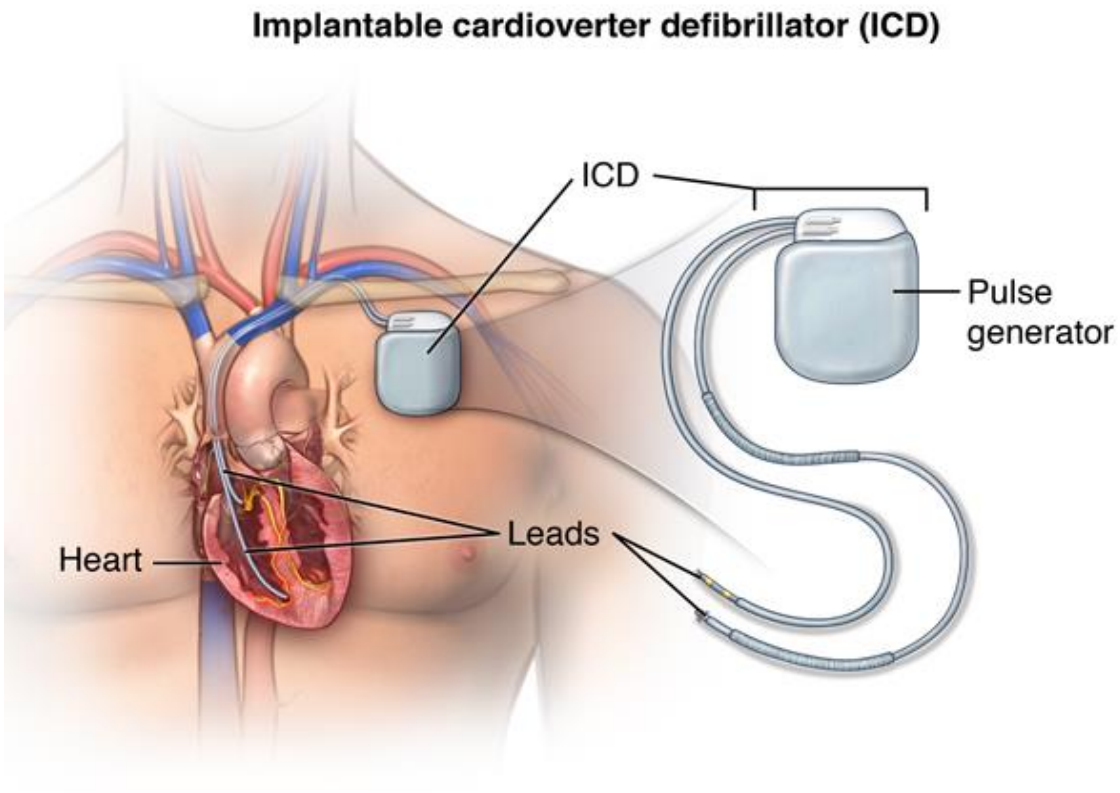

Figure 7: Implantable cardioverter defibrillator(ICD)

c) What are the components of a pacemaker/ICD

Pacemaker Compose three main parts:

• A beat (pulse) generator with a sealed lithium battery. It makes the electrical signals that make the heartbeat. Most of them can also receive and respond to signals sent by the heart itself.

• Wires (leads): leads are insulated flexible wires which conduct electrical signals between the heart and the pulse generator. One end of the lead is connected to the pulse generator and the electrode end of the lead is positioned in the heart.

• Electrodes: they are found on each lead.

d) How it is work

The important part of this whole thing is an ecosystem(A digital healthcare ecosystem is an infrastructure that supports the shift from an organization-centric to a patient-centric model of delivering healthcare services using digital platforms.) and so the way these are set up within the patient's home on the bottom left actually its patient monitoring system. Most of these sit at the nightstand the device communicates to that usually at night when the patient's sleeping. Because it's gathering data and sending it up through the network over the patient care network that way the manufacturer can monitor it. But more importantly, the physician can give indicators for that patient.

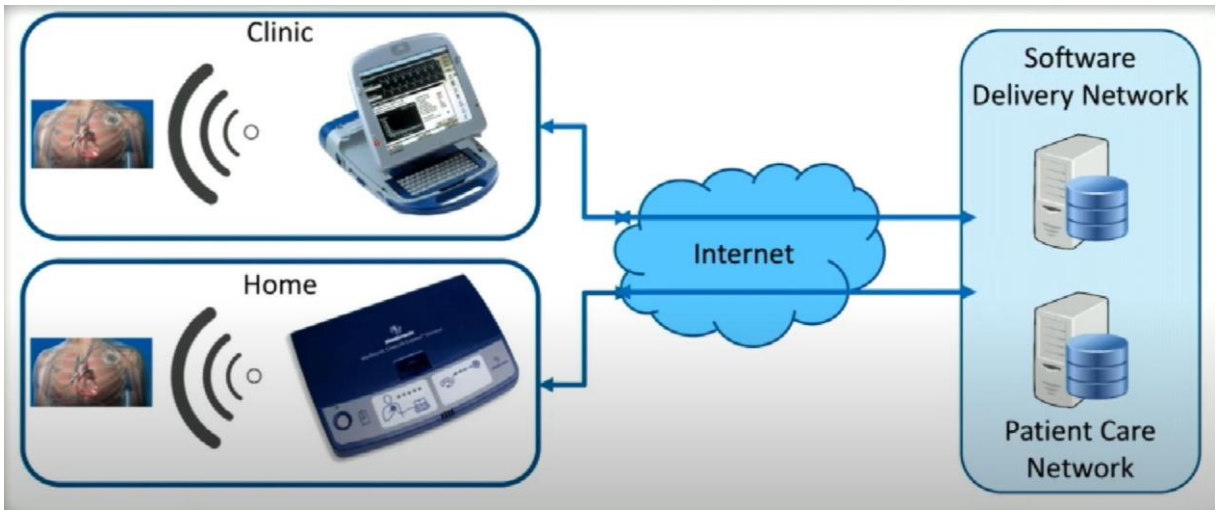

Figure 8: EcoSystem

Another part of the ecosystem is the actual programmer itself that's it at the clinic and that's what the physicians will use to actually program the therapy that goes into the Pacemakers and so that it's done over a radio frequency communication they will program when it's supposed to talk about what the pacing algorithm is and a whole set of parameters for that patient.

Also, There is the backend piece of it which is also part of this ecosystem as the SDN or the software delivery network so this is where updates are actually pushed down to these devices or from the perspective of the patient care network which is also back in the manufacturer where that data is brought in.

The important thing to understand at the top left-hand corner of the picture. This is a physician programmer these things also have the by design capability to update the firmware on the device itself. So not only is there a program on the pacemaker or ICD that says this is what the pacing cadence should be, this is the criteria to deliver a shock to get someone's heart started.

This thing also has software on it as well. The programmer adjusts the therapy that you're getting and can also change the software on the device by design.

e) How do can attacks happened?

Attacks against radio communications can hurt the user at home, in the clinic, and outdoor settings. These attacks can be targeted against single patients.

Figure 9: Home Monitoring Device

1- When we look at these the actual programmer themselves the various devices. if we look at radio communications and this is what some of the past research is alluded to, you can target a single patient using RF, that's kind of the one-to-one scenario. Hackers can launch an attack against one specific individual.

If we look at the home monitoring station if the attacker can go to someone's house and target that specific home monitoring system he can do a one-to-one attack.

2- Attacks against the programmers can attack a patient in the clinic. These attacks can also update firmware on the implanted device, allowing for more persistent attacks. These attacks can be targeted against single/multiple patients.

Figure 10: Programmer clinic Device

To be clear the programming is a little different it's kind of one to multiple. Because that programmer sits in a physician's office or an operating room or clinical setting and those devices will program multiple ICD. Those programmers might be responsible for dozen one hundred more and there's about ten thousand of these in the world.

The programmers run Windows XP operating system. (Yes, Windows XP)and you can imagine the number of vulnerabilities in a system like this.

The researcher's possible attacks hinge on things like connecting to HTTP web servers over the internet or manipulating wireless radio signals.

3- Attacks against the SDN can impact the entire ecosystem. the attack can be targeted against all patients

these are the most interesting attacks though. Therefore there's a mechanism a communications path from these devices through the Internet to servers that are basically internet basing. If someone were to exploit these components in its current situation this is where you can attack every patient. Because you would have access to update the software on the whole monitor even the programmer software. Also if you have access to a programmer you can have influenced the software on the programmer what can you do you can by design change therapy and you can by design change software on the actual pacemaker or ICD.

When you look at the threat model you know that the radio-based exploits are easy attacks against the actual programmer itself. If any part of this gets compromised the potential for every single one of your patients to get hurt or killed is present. To be clear not every vulnerability allows that but if someone compromises your software delivery network and you don't have the right mechanisms in play they will be able to leverage that to influence every single programmer in the field. Also if they can influence every programmer in the field they can reprogram the therapy and the software on every single device in the field.

So these parts are the riskiest parts of the threat model.

Related Researches:

Other supporting research has been published in the past years that highlights security risks associated with the implantable cardiac device ecosystem:

1- In 2008, Halperin et al. evaluated the security risks and presented the attacks on the IMDs, and how they can improve patient data privacy from theft, and how to design secure devices. The research demonstrates reverse engendering the ICDs communication protocols and use software define radio to launch an attack and impact the patient safety.

2- In 2012, the director of embedded device security for computer security firm IOActive Barnaby Jack could develop software that allowed him to remotely send an electric shock wave to anyone put a pacemaker within a 50-foot radius. He demonstrated live at the BreakPoint security conference in Melbourne how to deliver a deadly electric shock. Unfortunately, jack died and the video of the demonstration is not available because he did not want to mention the name of the manufacturer and put anyone to danger.

The problem is not restricted to just pacemakers. At the McAfee FOCUS 11 conference in October 2011, he accessed an insulin pump (without its serial number) through its radio link and used it to deliver a fatal dose.

After this huge amount of danger to patient safety, how do we can mitigate these Risks?

7. Technical Solutions

This Some Steps That you need to ensure the safety of the System from getting Hacked. The major vendors employ a similar architecture framework, device intercommunications, including communication protocols, embedded device hardware, and device authentication mechanism. The Most Risk as we mentioned in the previous attack was from the underlying protocols and system-system communications.

To mitigate potential risk to patient care, it is recommended that healthcare providers evaluate their respective implementations and approve that effective security controls are in place to protect against identified weaknesses that may lead to potential system hacked.

1- Patching The Systems

As we mentioned in the past section that some companies in healthcare especially are steal using unpatched systems such as Windows XP, Windows 7 or even using unpatched software which will lead to Remote code execution on this device.

To be clear a security patch is a change applied to an asset to correct the weaknesses described by a vulnerability. This remedial action will prevent successful exploitation and eliminate or mitigate a threat's ability to exploit a critical vulnerability in an asset.

The patch management process is a part of vulnerability management – life cyclical which: identify the weakness, classify, remediate, and mitigating vulnerabilities.

Security patches are the primary method of fixing security vulnerabilities in software or system. Today, Microsoft releases its security dedicated patches once each month, sometimes less than that. Other operating systems and software projects have security teams committed to releasing the most reliable software patches as soon as possible after a vulnerability announcement. Security patches are closely tied to responsible disclosure.

These security patches are critical to ensure that the business process does not get affected. In 2017, companies were struck by a ransomware called WannaCry(we will get more details about it later) which encrypts files in certain versions of Microsoft Windows and demands a ransom via CryptoCurrency. In response to this, Microsoft released a patch that stops the ransomware from running but is sure that every day there is new ransomware is released which No one can prevent permanently. We, Will, discuss more solutions on how to prevent ransomware Viruses.

2- Secure all device From Scratch:

The best way to secure a medical device is to secure it from the beginning of the creation: These are Some Greate Points that can help to produce more secure IOT Devices:

- **Is external USB on the monitoring device at home restricted to only allow communication between authorized devices? Implement Security Control Policy.**

- **Where The credentials are saved in the home monitor or the programmer device? Must be in a safe place and use API to authenticate remotely then use TokenID to Login With.**

- **Where is the data of the patient is store in-home monitor device or programmer device? how it was stored? The Best way is to store the data in an external place encrypted.**

- **If the Home monitor Device receives a remote firmware update, How does the authentication happened? Configure security control policy to authenticate the source of the firmware update.**

- **Check if authentication is required when the programmer wants to program an ICD.**

- **Putting Security Control on home monitoring Device to prevent it from transmitting commands to implantable cardiac device program.**

- **How are assess The security Controls That are implemented?**

3- Secure the RF Communications

Many health providers are not yet considering the RF activities in their workspace because they are thinking that all radio communications are encrypted. Regardless IoT devices are more vulnerable to attacks.

It's still common nowadays to find radio protocols working in unencrypted ways or with common or reused key identifiers that can be easy to decrypt. That means that not only can an RF attacker listen to IoT traffic, they can also send arbitrary commands to force the device to do something malicious. The radio attack can be done from a mile away using antennas and amplifiers. As, we demonstrate in the previous section.
So The Important Thing in Security is the Privacy of the data. Cryptographic implementation is one of the most important tasks in securing the sensor data on IoT devices. From These operations:

- Encryption and decryption.
- Key and hash generation.
- Verify hashes.

That is the most used tasks to assure data privacy.

When designing IoT devices we must care about three things:

- Security
- Low Costs
- Performances

The Best Way to secure IoT devices by using Lightweight Cryptography.

a) Lightweight Cryptography:

Lightweight Cryptography is a cryptographic algorithm or protocol suits for implementation in constrained environments. It is used in many fields such as :

• Sensor Networks.
• Healthcare IoTs.
• Radio Frequency identification.
• Smart Grid.
• IoT Distributed Control Systems

Lightweight Block Cipher:

Orange Company, Ruhr University and Technical University of Denmark developed it. This some characteristics of it cipher:

• Compact Size - 2.5 times smaller than AES
• Block Size: 64 bits
• Key Size: 80 bit - 128 bit
• Low Power Consumption
• High Chip Efficiency

Performance Analysis of Lightweight Cryptography:

• Cost Effective
• Reliable
• Size Effective
• Small Key Size

b) One Time Password Authentication for IoT:

in 2015, Experts such as V L Shivraj - M a Rajan have shown That's possible to use one Time Password and they have demonstrated how these algorithm works and the benefits added to security by it. Why OTP is Good Security Choice for IoT device:

• It Focusing on lightweight Authentication Methods For IoT and Users.
• It used some of the principles in lightweight identity-based Elliptic Curve Cryptography.
• OTP is a mix of Numbers and Characters used to validate the user session.
• OTP used for a single Login session, So is more secure than the Normal Password.
• Encrypt the OTP in two ways: sending it to the client and decrypt it when receiving it from the client to check if are same
• There are two parts in this architecture: one is the hardware design, and the Other is OTP and Encryption.
• They Used AES Encryption algorithm to encrypt OTP

8. General Solution

Paul Chichester Director Operations of the National Cyber Security Centre of Operations, said: [paul chichester]
“Protecting the healthcare sector is the NCSC’s first and foremost priority at this time, and we’re working closely with the NHS to keep their systems safe. By prioritizing any requests for support from health organizations and remaining in close contact with industries involved in the coronavirus response, we can inform them of any malicious activity and take the necessary steps to help them defend against it."

1- The Health Care organizations Work with Security Experts :

As we said earlier, the companies making devices are totally medical device makers, which might not be familiar with security and threats. Most experts agree that any possible solution begins with getting Security Professional to work with healthcare providers, in order to clarify the value of all infrastructure and technologies around the medical field.

2- Launch Bug Bounty Programs

A bug bounty program is a deal offered by many websites, companies, and software developers by which individuals can receive acknowledgment and compensation for reporting bugs, especially those concerning security exploits and vulnerabilities.

These programs provide developers to discover and fix bugs before the general public can find them, preventing incidents of widespread damage. Bug bounty programs have been implemented by a lot of companies, including Google, Reddit, Mozilla, Facebook, Yahoo, Square, Microsoft, and the list go so long. Bug bounty and vulnerability disclosure programs have been proven to produce excellent results in finding and fixing vulnerabilities.

White hat hackers(security researchers) are always looking for vulnerabilities, whether invited or not cause the hacker always Curious about how things work. it's smart to proceed toward the infosec work of this sort carefully and structure the program in a way that does not endanger your organization or patient data. Bug bounties can increase in-house security staff, as well as validate in-house security efforts.

The groups (APTs) operating in the dark world of cybercrime are studying new ways and techniques to penetrate Those systems and devices. So healthcare organizations, too, need to stay ahead of the game by examining new solutions available. It commendations any mature security program, filling the gap left by scanners and exponentially improving the probability of finding good results.

Conclusion

after the amount of increase in Internet of things Devices. Especially in the Healthcare field, It is important to take into consideration the security Side. Cyber Security is essential to secure the data and the privacy of people in general and patients in special. We discussed in this paper the most dangerous types of attacks that could kill any patient, and we presented many solutions that sought to significantly reduce the risk of attacks.

Resources

- W. Burleson and K. Fu, Design Challenges for Secure Implantable Medical Devices, Proceedings of the 49th Annual Design Automation Conference, 2012.
- D. Halperin, T. Heydt-Benjamin, B. Ramsford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno and W. Maisel, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008.
- X. Hei, X. Du, J. Wu and F. Hu, Defending Resource Depletion Attacks on Implantable Medical Devices, Proceedings of the 2010 IEEE Global Telecommunications Conference, 2010.
- Security, H. N. (2020, April 7). *Radio frequency: An invisible espionage threat to enterprises*. Help Net Security. https://www.helpnetsecurity.com/2020/04/08/radio-frequency-threats/
- Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015). One time password authentication scheme based on elliptic curves for Internet of Things (IoT).

2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW). Published. https://doi.org/10.1109/nsitnsw.2015.7176384

- E. Marin, D. Singelee, F. Garcia, T. Chothia, R. Willems, B. Preneel, On the (in)Security of the Latest Generation Implantable Cardiac Defibrillators and How to Secure Them, Proceeding of the Annual Computer Security Applications Conference, 2016.
- Storm, D. (2011, August 4). *Black Hat: Lethal Hack and wireless attack on insulin pumps to kill people*. Computerworld.
- Franzen, C. (2013, October 22). *Dick Cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering*. The Verge. https://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007
- Peterson, A. (2013, October 21). *Yes, terrorists could have hacked Dick Cheney's heart*. Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/