IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

MITIGATING CYBERSECURITY RISKS IN MEDICAL DEVICES USING SECURE IMPLANTED TECHNIQUES

[1]Nasmin Jiwani, [2]Ketan Gupta

[1,2]Research Scholar

[1,2]Department of Information Technology

[1,2]University of The Cumberlands, Kentucky, USA

Abstract: Cyberattacks on medical groups endanger patient care. When medical devices depend on poorly maintained legacy applications that cannot change and may contain publicly reported vulnerabilities, the threat of being victimized through a destructive attack increase, the purpose of this study is to give perspective on strategies found in the literature that minimize risk induced by legacy software on medical equipment. Techniques considered include special strategic Bluetooth connection via mobile phones, anomaly detection based on behavior, and signal authentication using a physical attribute. Such methods are suitable for many use-cases, from pacemaker security to healthcare sensor nodes. Many solutions rely on intrusion identification and tunneling unencrypted Bluetooth communications. Those techniques have different application areas, and the best choice depends on the kind of medical equipment. This study describes a solution to the security of software shim, which can be embedded in any medical device and used to minimize current cyber threats as well as future. Rather than specific code, the paper provides a general solution. The coding would be distinct to each device. These firmware solutions can address security issues with any implantable healthcare device.

Index Terms – Cybersecurity, Healthcare, Medical Devices, Cyberattack, Legacy Software.

I. INTRODUCTION

Cyberattacks have become more common in the healthcare sector in recent years. Ransomware attacks on hospital services have resulted in substantial monetary losses and harmed patient management. Furthermore, healthcare security breaches charge the sector billions of dollars, adversely affect patient confidentiality, and enable widespread identity fraud. Intruders have observed that the health care system is an appealing target: health data on the black market could be ten times more expensive than credit card numbers, for example, as it can be used to obtain drugs or commit insurance fraud. Illicit attempts against hospitals have also proved to be successful. Attackers have compromised medical equipment in clinics like blood gas monitoring systems, MRI scan devices, and X-Ray tools [1]. These gadgets have since been used as a launching pad to wander across medical centers laterally. 'Physical ransomware' might be employed in the future to disable vital (healthcare) hardware implicitly. A scandal in which an Austrian restaurant was aimed by a pressure of ransomware which deactivated keys to the room and retained all doors closed till a ransom was paid, demonstrates the feasibility of such an attack.

Moreover, threats in healthcare devices, such as mobile infusion pumps and implantable cardiac equipment, have allowed intruders to impact patients wirelessly [2]. Cyberattacks have become more common in the healthcare sector in recent years. Ransomware attacks on hospital services have resulted in substantial monetary losses and harmed patient management. Furthermore, healthcare security breaches charge the sector billions of dollars, adversely affect patient confidentiality, and enable widespread identity fraud. Intruders have observed that the health care system is an appealing target: health data on the black market could be ten times more expensive than credit card numbers, for example, as it can be used to obtain drugs or commit insurance fraud. Illicit attempts against hospitals have also proved to be successful. Attackers have compromised medical equipment in clinics like blood gas monitoring systems, MRI scan devices, and X-Ray tools [1]. These gadgets have since been used as a launching pad to wander across medical centers laterally. 'Physical ransomware' might be employed in the future to disable vital (healthcare) hardware implicitly. A scandal in which an Austrian restaurant was aimed by a pressure of ransomware which deactivated keys to the room and retained all doors closed till a ransom was paid, demonstrates the feasibility of such an attack. Moreover, threats in healthcare devices, such as mobile infusion pumps and implantable cardiac equipment, have been demonstrated, allowing intruders to wirelessly impact patients [2].

Medical devices are incredibly prone as they commonly lack basic security protocols and operate legacy operating systems and software with widely known risks [3]. This is due to aging equipment that no longer gets technical support or the complexity of implementing spots to devise software. Fixing medical equipment can be especially difficult due to certification requirements: for instance, whenever an update to a CE-approved device is considered a significant recompilation, comprehensive testing is required before the pattern can be issued. When patching is not an option, the fundamental solution of substituting the susceptible hardware ultimately can be extremely costly. As a result, we want to trace other alternatives to the privacy problems that arise when a health professional is forced to depend on healthcare devices running legacy software [4].

We want to identify and classify literature related to the research question: what alternatives, apart from complete replacement, identify safety challenges posed by legacy software in healthcare equipment? For such analysis, we took systems that perform interaction and computation that meet the description of a medical device' which is equipment aimed to be employed for medical uses. We want to identify and classify literature related to the research question: what alternatives, apart from complete replacement, identify safety challenges posed by legacy software in healthcare equipment? For such analysis, we took systems that perform some interaction and computation and meet the description of a medical device' which is equipment aimed to be employed for medical uses.

II. METHODOLOGY

Method and analysis, which are commonly used, are listed here.

STRATEGIES FOR INTRUSION DETECTION

The method for dealing with legacy software is to implement a different outer surveillance system that attempts to predict if a machine is being attacked. While such a process doesn't defend against threats on its own, it does help patients or specialists quickly respond, for instance, by turning off the machine [5]. An IDS (intrusion detection system) is a type of monitoring system. An IDS must be capable of monitoring a few characteristics of the machine to be secured (e.g., contents of a message or physical attributes of a wireless link) and for it to use detection method to distinguish between normal and malicious behavior [6].

We categorize detection techniques into three groups:

• Knowledge-based: The intrusion detection system will identify prespecified annotations of known threats. It will be unable to locate threats that seem to be unconfirmed or not present in the attack directory of the IDS.

• Behaviour-based: the Intrusion detection system would then recognize how a machine performs under normal circumstances and will generate a warning if it detracts from this. It can detect non-predefined attacks. But this kind of IDS is more susceptible to false-positive than just a knowledge-based IDS, as abnormal behavior does not indicate an attack.

• Based on Behaviour-specification: The IDS is precompiled by such a configuration of how well a machine needs to behave and detect deviations from such specification. This will not change its definition dynamically of what activity is appropriate, apart from behavior-based frameworks. The false positive and negative rates are calculated by the exactness of the configuration, which must be defined manually for each device [7].

When a privacy activity is authorized, an IDS must respond in a certain way. Generally, it shows an alert to an organization's security operation center; however, it might not be satisfactory when a patient takes a medical device home. When the response includes actively interfering with the supervised system to thwart the attack, the IDS is regarded as an intrusion prevention system (IPS). We discovered that the methods regulate various aspects of a medical device or its surroundings to locate suspicious behavior. We found that every option controls one of the following medical equipment components: IMD physical actuators, implanted medical device (IMD) wireless communications, IP network packets, sensor network node readings, or software execution characteristics [8].

1. IMD WIRELESS COMMUNICATIONS MONITORING: Research suggested a specialized intrusion detection system (IDS) and intrusion prevention system (IPS) to secure on-body devices to communicate. They go by how a human's tissue and body shape affect radio propagation properties to determine if a signal is being sent through an on-body machine. It is regarded as malicious if the signal is instead sent via air from a range.

2. CHECKING READINGS FROM SENSOR NODES IN THE NETWORK: The researcher developed an IDS that generates sensor biometrics and operates noise that identifies each sensor uniquely. This enables sensors to be recognized even if an existing routing protocol does not endorse (strong) confirmation. This presumes how an attacker's spoofed measured value has a different sound fingerprint.

3. SOFTWARE EXECUTION FEATURES MONITORING: The methods consider device software to be a black box whose inputs and outputs can be supervised. It directly controls the software execution in this approach. It is accomplished by joining a tracking system to a pre-existing system exposed to trace (such as a pacemaker). This enables monitoring software clock properties impacted by events such as cache misses, branch mispredictions, and interrupts. Support vector machine learning can distinguish between typical software execution characteristics and anomalies induced by an attack [9].

METHODS FOCUSED ON INDISCRIMINATE JAMMING:

This is due to defects in a network protocol used primarily by implantable cardiac defibrillators (ICDs). Countermeasures are described that can be used quickly with no need to retrieve established ICDs. The criterion is for the device programmer to continuously mash the wireless connections that the ICD likes to listen to whenever the developer is not interacting with the ICD on its own. The said option doesn't try to provide intrusion detection or access control. Instead, it tends to take advantage of the opportunity that the programmer activates all interactions under this use case. This would not entirely prevent attacks; however, it does limit the time frame in which they'll be conducted [10].

SECURE REMOTE MAINTENANCE SOLUTION:

Researchers suggested enhancing an existing health device with highly secure capabilities. The machine still had a software-enhanced version, over which the researchers constructed an application-based module which was also deliberately designed to not tamper with the device's primary functions (thus eliminating the need for re-certification) and not bringing in new vulnerabilities. The maintenance component would be linked to an assistance server via a verified and encoded VPN tunnel, preventing unauthorized attackers from intercepting communications. On the other hand, the primary device would have no visible network connections on the basic device. This implies that a channel attacker could not exploit vulnerabilities in the primary device (presuming a safe maintenance component) [11].

III. PROPOSED SOLUTION

This paper describes the suggested SIMD (Secure Implanted Medical Device) system in detail. The SIMD is a module that could be integrated into existing healthcare devices. It can be applied to a diverse range of medical products. The main feature of this framework is that any medical device developer can quickly install it. As a result, it can be used to reduce current security flaws.

Problem Addressing:

As this paper demonstrates, there is widespread concern about the safety of medical devices. Various errors in medical devices have been discovered. The FDA has recently issued an alert about the security of such devices. This study gives information about a project that aims to provide a solution to such security issues.

Overview of System:

The suggested scheme is a shim of software that could be incorporated into almost every device's firmware to reduce cyber threats. A simple code fragment embedded to apprehend API (Application Program Interface) is called a software shim. In some instances, the shim might change those calls. This is used occasionally for data formatting or to connect various protocols. The SIMD system shim could intercept and analyze any commands communicated to the medical device to ensure conformance with safe operational metrics.

A software shim option has been opted for as this could be incorporated into a current device without requiring considerable changes to the current device's firmware. All known attack matrices for implanted healthcare devices rely on device communication. As a result, monitoring and inspecting those information exchanges is an analytical place to put security in place.

The suggested SIMD system has the following characteristics:

- Only validated data can be transmitted to the medical device.
- Only reliable and valid devices can access medical data.
- All dosage data is validated against acceptable standards.

This is a high-level overview of features, and each section will elaborate on his. The illustration below describes a use-case diagram showing how various accessors will communicate through the SIMD system. The problem that this suggested scheme attempts to solve is securing the activities featured in the use case. The aim is to ensure efficient cyber threat mitigation.

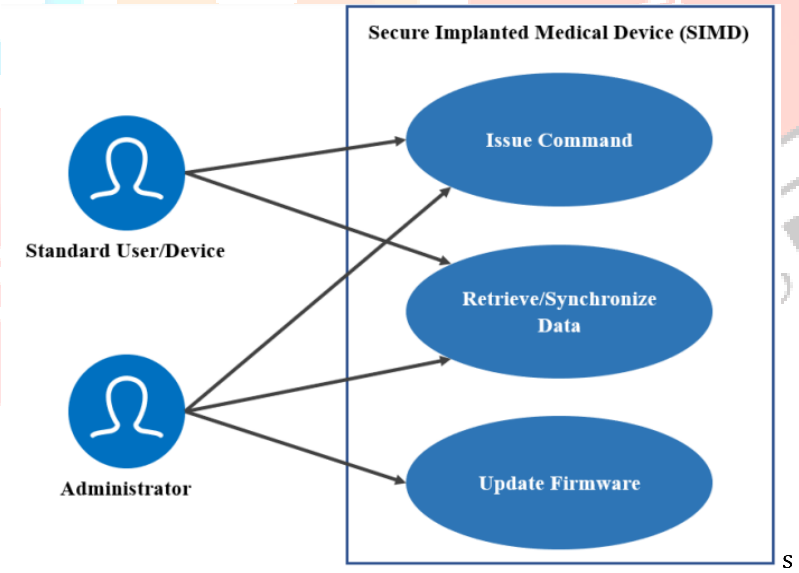
Secure Implanted Medical Device (SIMD)
Standard User/Device
Administrator
Issue Command
Retrieve/Synchronize Data
Update Firmware
s

Figure 1. SIMD Use Case

System Specifications:

The suggested scheme will combine multiple security features into implanted medical devices to mitigate various threats. These changes, in addition to resolving security issues, will enhance privacy concerns for such medical equipment.

Medical device safety is primarily concerned with two issues.

- Incorrect data and commands are being sent to the medical equipment by mistake or with destructive intent.
- An unauthorized user extracts data from the medical equipment.

The suggested SIMD system uses conventional and proven techniques to ensure operations security. The proposed framework will be added as a coding unit for any medical industry. The steps are as follows:

The addition of the code library will support the following tasks:

- Keeping a whitelist of healthcare equipment permitted to communicate with the healthcare equipment under consideration.
- Inspecting the whitelist before accepting any action.
- Ensuring that any data update, request, or command is digitally signed before operating.
- Assuring that such activities do not tamper with the device's everyday activities.
- Keeping track of all required tasks.
- Send notifications whenever required.

There are two methods for validating communication with medical devices. Initially, the healthcare industry would include a set of devices with which it is preparing to communicate. This whitelist would contain the practitioner's node and other approved devices. Any commands received from machines not included on the whitelist might be refused. Moreover, communications signed digitally by an authorized origin will be supported only. The integration of whitelisting and digital signatures will allow for strong authentication of any connectivity. Communications have the provision of both instructions and data requests. Every device would also contain appropriate clinical parameters in the SIMD system shim. Insulin levels, heart rate, and other pertinent medical operating parameters are examples of medical parameters. All commands received will be analyzed to such medical factors. Commands that go beyond these specifications will be rejected and logged. It may also be set to inform both the health professional and the user about the incident.

Finally, there will be a secure manner on the medical device. In essence, if an attempt is made to disrupt the healthcare device's safety, the device will enter a most petite mode of operation. In this approach, the device would dismiss any command that came wirelessly and was unrelated to the device's normal daily functions.

The SIMD system code component intercepts each operation. The module's function is described in detail below.

Action	Responsibility of SIMD Module
Issue of Command	As the medical device receives a command. The SIMD system module needs to perform three tasks: 1. Confirm that the command is coming from a device upon that authorised whitelist. 2. Verify that the command text was signed digitally with a correct digital signature. 3. Confirm that the command does not violates operating features.
Data Transfer Request	The medical device receives a request for synchronization or for data transfer. The SIMD module must perform two tasks: 1. Confirm that the command is coming on the authorised whitelist from a device. 2. Verify that the command message was signed digitally with a current and valid digital signature.
Firmware Update	A plausible updation is delivered to the medical device. The SIMD module must perform two tasks: 1. Confirm that the command is coming on the authorized whitelist from a device. 2. Verify that the command message was signed digitally with a current and valid digital signature.

Table 1. Module Operation

Operation Modes: The SIMD module operates in two modes. The first phase is known as usual. In this mode, all features are accessible. The 2nd mode is known as an emergency. If an attempt is taken to breach the system or any hardware or software problem, the device will stop accepting software commands or updates and only allow data synchronization. The prevailing system can be integrated into established healthcare devices like insulin pumps, pacemakers, and other devices. As a result, it will be applied to a human subject. But extensive testing will be required before such implementation. The suggested framework would enhance the safety of current healthcare devices and could be incorporated into new ones. There is, however, an extra computational complexity. During progression, measures must be taken to ensure that it will not tamper with the prime role of the healthcare equipment in question.

The SIMD module will indeed improve existing health devices in the following ways.

- Ensuring that any command originates via a reliable source.
- Ensuring that any update is from a credible source.
- Ensuring that any command falls inside permissible limits.
- A lower operational mode in the event of an emergency.

IV. CONCLUSION

We discovered the risks posed by legacy software in healthcare devices. Those are all mainly based on intrusion detection or the allocation of secure communication tunnels. They offer a good range of alternatives for dealing with insecure equipment whose software cannot be modified. Most of such solutions are centered on embedded and wearable devices that communicate wirelessly or on sensor networks which are a component of a broader system. The strategies can be implemented by introducing new hardware on top of legacy devices, tracking communications through an intermediating system, upgrading programmers, or utilizing pre-existing application add-on interfaces. We noticed that each solution uses a different set of application areas and attacker concepts, which means that the best choice depends heavily on the kind of medical equipment that needs to be protected. Intruders can circumvent some tunneling techniques, and usability issues have also been recognized in strategies requiring extra hardware. Moreover, IDS still needs to be experimentally tested independently.

Future studies may discover much about the efficacy of such solutions and how to enforce them in real. This study also describes a security solution based on software shim that can be embedded in any medical device and used to minimize current cyber threats and the future. Rather than specific code, the paper provides a general solution. The coding would be distinct to each device. If legacy-compliant security techniques are integrated into security tools, medical institutions will get more possibilities to strengthen security despite legacy medical equipment whose software cannot be modified. The majority of such solutions are centered on embedded and wearable devices that communicate wirelessly or on sensor networks which are a component of a broader system.

The strategies can be implemented by introducing new hardware on top of legacy devices, tracking communications through an intermediating system, upgrading programmers, or utilizing pre-existing application add-on interfaces. We noticed that each solution uses a different set of application areas and attacker concepts, which means that the best choice depends heavily on the kind of medical equipment that needs to be protected. Intruders can circumvent some tunneling techniques, and usability issues have also been recognized in strategies requiring extra hardware.

Moreover, IDS still needs to be experimentally tested independently. Future studies may discover much about the efficacy of such solutions and how to enforce them in real. This study also describes a security solution based on software shim that can be embedded in any medical device and used to minimize current cyber threats and the future. Rather than specific code, the paper provides a general solution. The coding would be distinct to each device. If legacy-compliant security techniques are integrated into security tools, medical institutions will get more possibilities to strengthen security despite legacy medical equipment.

VII. REFERENCES

[1] N. Jiwani, K. Gupta, and P. Whig, “Novel HealthCare Framework for Cardiac Arrest With the Application of AI Using ANN,” in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, 2021, pp. 1–5, doi: 10.1109/ISCON52037.2021.9702493.

[2] N. Jiwani, K. Gupta, and N. Afreen, “Automated Seizure Detection using Theta Band,” in *2022 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2022, pp. 1–4, doi: 10.1109/ESCI53509.2022.9758331.

[3] N. Jiwani, K. Gupta, and N. Afreen, “A Convolutional Neural Network Approach for Diabetic Retinopathy Classification,” in *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)*, 2022, pp. 357–361, doi: 10.1109/CSNT54456.2022.9787577.

[4] K. Gupta, N. Jiwani, and N. Afreen, “Blood Pressure Detection Using CNN-LSTM Model,” in *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)*, 2022, pp. 262–366, doi: 10.1109/CSNT54456.2022.9787648.

[5] K. Gupta, N. Jiwani, N. Afreen, and D. D., “Liver Disease Prediction using Machine learning Classification Techniques,” in *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)*, 2022, pp. 221–226, doi: 10.1109/CSNT54456.2022.9787574.

[6] S. K. B. Sangeetha, N. Afreen, and G. Ahmad, “A Combined Image Segmentation and Classification Approach for COVID-19 Infected Lungs,” *J. homepage http//iieta. org/journals/rces*, vol. 8, no. 3, pp. 71–76, 2021.

[7] N. Nasir, N. Afreen, R. Patel, S. Kaur, and M. Sameer, “A Transfer Learning Approach for Diabetic Retinopathy and Diabetic Macular Edema Severity Grading,” *Rev. d’Intelligence Artif.*, vol. 35, pp. 497–502, Dec. 2021, doi: 10.18280/ria.350608.

[8] N. Afreen, R. Patel, M. Ahmed, and M. Sameer, “A Novel Machine Learning Approach Using Boosting Algorithm for Liver Disease Classification,” in *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, 2021, pp. 1–5.

[9] Sharif, M. H. U. (2022). Web Attacks Analysis and Mitigation Techniques. International Journal of Engineering Research & Technology (IJERT).

[10] R. Chourasiya, V. Patel, and A. Shrivastava, “Classification of cyber attack using machine learning technique at microsoft azure cloud,” Int. Res. J. Eng. Appl. Sci, 2018.

[11] U. K. Kachhwaha and A. Shrivastava, “CREDIT THREAT ESTIMATION BY MACHINE LEARNING TECHNIQUES OVER CLOUD PLATFORM,” 2020.