Cybersecurity Analysis for a Remote Drug Dosing and Adherence Monitoring System

Dino Mustefa[1,2][0000−0002−9453−2838] and Sasikumar Punnekkat[2][0000−0001−5269−3900]

[1] Embedded Systems, ALTEN Sweden AB, Stockholm, Sweden
[2] Mälardalen University, Västerås, Sweden
dino.mustefa@mdh.se, sasikumar.punnekkat@mdh.se
https://www.alten.se, https://www.mdh.se

Abstract. Remote health monitoring and medication systems are becoming prevalent owing to the advances in sensing and connectivity technologies as well as the social and economical demands due to high health care costs as well as low availability of skilled health care providers. The significance of such devices and coordination are also highlighted in the context of recent pandemic outbreaks underlying the need for physical distancing as well as even lock-downs globally. Though such devices bring forth large scale benefits, being the safety critical nature of such applications, one has to be vigilant regarding the potential risk factors. Apart from the device and application level faults, ensuring the secure operation becomes paramount due to increased network connectivity of these systems and services. In this paper, we present a systematic approach for identification of cyber threats and vulnerabilities and how to mitigate them in the context of remote medication and monitoring devices. We specifically elaborate our approach and present the results using a case study of an electronic medication device.

Keywords: Medical IoT · Cybersecurity · Safety · Remote eHealth solutions · Medicine dosage · Remote adherence monitoring.

1 Introduction

Advanced communication technologies are already an integral part of health services. As smart devices grow in number and equipped with advanced emerging communication technologies, they will be able to communicate directly (device-to-device) and to cloud based health services (device-to-cloud) via either a base station or a gateway. They will form the medical internet of things (MIoT) and will provide diagnostic data access to remotely located disease management system over the internet. This will enable patient mobility and remote medication capabilities as well as continuous adherence monitoring among other interesting applications and possibilities. Though this will bring interesting applications into the medical domain, there is also a great risk that these devices become vulnerable to cybersecurity attacks by adversaries as they are connected to the internet which in turn can put the safety of patients in danger.

Safety practices in critical solutions in the domain are well established and prescribed by safety standards[3]. These standards state clearly how systems should be developed, verified and maintained to minimize risks of accidents and failure over the lifetime of a product. Yet, established safety practices fall short of addressing the new cybersecurity threats and system vulnerabilities that can originate from the growing connectivity and addition of new smart communication technologies and grid components. There are no standards yet on how to deal against these inevitable cybersecurity threats and device vulnerabilities to adversary attacks, but there are guideline documents[4][5] that provide recommendation on what to consider and which controls to implement to reduce the risks and to guard patients from any potential danger. For wider adoption of these devices and their enhanced communication features, it is necessary to do cybersecurity related risk assessment and to mitigation the risks in order to guarantee dependability of health services so that users can rely on them.

The goal of this research is to help creating trustworthy remote medication monitoring system involving intelligent oral medicine dosing device. We have proposed an approach for a detailed cybersecurity threat identification, analysis and mitigation. Following that, we have performed a detailed study on identifying potential threats and vulnerabilities in the system. The investigation covers all system components and scenario including cybersecurity related risks during hardware (HW) and software (SW) design and development (production flow of the HW and SW), distribution (packaging and transportation to end customer), maintenance and post-distribution phases of the product. We have also investigated all network related cybesecurity threats. Finally, we performed an investigation on how cybersecurity preventive strategies can be improved to guard the device against threats that can exploit vulnerabilities in the device as well as on how the device can continue to function despite the system is exposed to a cyber attack.

The paper is organized as follows. Section 2 provides brief information in remote medication and monitoring solutions in general followed by more elaborated information on remote electronic medication and adherence monitoring devices and finally describes safety and cybersecurity challenges. The method and steps required to do threat identification and analysis will be explained in section 3. Section 4 provides description on the use case device and related safety and security challenges and the proposed approach will be used to do risk identification and analysis followed by possible mitigation solutions for identified critical risks. The conclusion remarks are given in Section 5.

---

[3] EN ISO 14971:2007 Medical device – Application of risk management to medical devices

[4] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, 2018

[5] FDA, Post market Management of Cybersecurity in Medical Devices, 2016

2   Remote Medication and Adherence Monitoring

According to [9], figure of world population aged 65 and above will be doubled in 2025 relative to the figures in 1990. The European population projection in 2012 [7] shows that this will keep on increasing if life expectancy keeps on growing. The same states that the size of working-age population in some regions of Europe will decline considerably including in health care domain. Altogether can have a great impact on the ratio of patients to health care personnel, which necessitates novel remote health care solutions for medication, monitoring as well as treatment purposes.

   Adherence is the degree to which a patient follows medication advice and guidelines. Poor adherence is a significant problem across all medical fields and one of the major causes of illness and of treatment failure, and limits providers' abilities to fulfill their ethical obligation of working to improve patients' health and well-being. Patients with chronic diseases and elders require continuous follow up to make sure that they are taking their prescribed medication properly. When patients do not respond to a certain prescribed medication, it can be difficult to determine whether the lack of response is due to nonadherence or whether the medication itself is not effective. [1] found a 76% discrepancy rate between what medicines patients were prescribed, and what medicines they actually took. Up to 25-50% of patients do not take their treatments as prescribed, threatening their health and well-being [2]. A quantitative review of 50 years of research shows; among patients with some disorders (e.g., schizophrenia, diabetes, asthma), nonadherence is the largest driver of relapse and hospitalization. Moreover, misuse or abuse and redirection of controlled substances is a major health issue, with over 50 000 deaths yearly in the USA[6]. In addition to the financial costs of nonadherence, patients who do not adhere to their medications face other potential serious consequences, including higher rates of complications and death. The cost of additional treatments and hospitalizations from nonadherence is estimated to be billions of dollars annually. Furthermore, clinical trials to assess the safety and efficiency of new drugs necessarily rely on proper medication adherence by study participants to obtain accurate data. Adherence or lack thereof has significant impact on the expected treatment outcomes and a significant cost to healthcare domain and society and leads to unnecessary suffering. Therefore, accurate assessment of medication adherence is both clinically important and challenging to all involved parties in the sector.

   Existing and emerging advanced smart sensors and connectivity technologies are core components behind a rapid growth of remote care delivery solutions. There are numerous eHealth devices out in the market where patients can medicate themselves with and report disease symptoms. These devices are equipped with smart sensors and advanced connectivity technologies [3] and can track medication activities and upload either the diagnostic data or just alerts to a remote central disease management system. This brings great values from personalized medication to remote adherence monitoring. But most importantly

---

[6] https://www.drugabuse.gov/related-topics/trends-statistics/overdose-death-rates

brings ability to make improved and fast decision by care givers or smart central disease management system as well as to provide feedback to patients through adjusting dosing size or doing a remote critical medical operations. In a bigger picture these solutions will bring many advantages like saving both time and resources, reduce the time required for diagnosis and treatment and reduce needs for hospitalization and emergency room visits. This will improve survival rate, especially to patients living in rural areas, and reduce health care costs both for patients and the health care organizations.

2.1   Remote Electronic Medication Adherence Monitoring

Traditionally, clinicians had to rely on patients' self-reporting of adherence to medications [5]. Studies show that self-reporting is unreliable: Patients may have inaccurate memories of taking their medications or may be embarrassed to admit failure to comply or inability to access (lack of finances, not understanding instructions, memory problems) medications. Scholars have pointed to the need for a more accurate measure of whether and when patients take their medications. Products that incorporate adherence monitoring are already on the market and others are awaiting FDA approval. There are different sorts of them:

1. Electronic medicine dosing device
2. Implanted and wearable body sensors [9]
3. Digital medicine: Proteus developed ingestible sensor[7].

Widely-used Medication Event Monitoring System (MEMS)[8] provides very high standard information about adherence. The electronic pillbox[9] is a simple electronic medication adherence tracking device based on a standards that overcomes some of limitations of previously developed similar products [4]. Proteus Digital Health developed ingestible sensor[10] that emits a weak signal when the medication is ingested and the signal is relayed via a patch worn on the abdomen that links with a smart-phone app and records that the medication was taken. eCare Companion[11] enables patient to enter medical information like blood pressure, etc. and fill answers to questionnaires about their timely health condition. This system communicates with sensor devices such as pulse oximeter, weight scale, blood pressure meter, and medicine dispenser to collect data automatically. Philips claims that they provide security and privacy protection of the patient's data, but do not provide details on mechanisms used.

Although *electronic medication devices* may not provide a direct or a complete evidence of medication ingestion as digital medicine does so, they can still

---

[7] https://www.proteus.com/how-it-works/

[8] https://www.aardexgroup.com/solution/MEMS-adherence-software/22

[9] http://www.med-tracker.com/

[10] https://www.proteus.com/how-it-works/

[11] https://www.usa.philips.com/healthcare/product/HC453564553051/ecarecompanion-patient-app-your-patients-gateway-to-care

provide enough amount of information related to medication adherence. On another hand, combining existing electronic medicine medication devices with an ingestible sensor or wearable sensors would improve efficiency of adherence report. Otsuka Pharmaceuticals' is working on combining ABILIFY (i.e., aripiprazole, which is currently FDA approved for a range of indications in the treatment of serious mental illnesses) with the Proteus ingestible sensor and uses an app to record patients' ingestion of their medication[12]. The app can also track, if the patient wishes, additional information such as self-reported mood and sleep ratings. What these devices have in common is automated collection of patient information, the ability to share that information with designated others, and the link to medication (ingesting a pill, signaling a dose of insulin).

Patients using electronic medication device can log symptom data or wearable sensors can track the state of disease activity and body response to medication, and link it to a connected system, have great potential to improve decisions making on right medication and right dosing which will enable better overall treatment decisions and better outcomes. In a connected system, these decisions can be made faster and simpler, saving both time and resources. Being able to track dosing and track a digital signal if medications are used outside the normal pattern or if the dispensing device is tampered with would allow healthcare and caregivers to act faster if misuse occur, and this feature in itself will have preventive impact on potential misuse.

2.2 Safety and Security Challenges

As MIoT products & solutions are getting cheaper and better, more and more patients will be heavily relying on them. To date, there are few accidents or disasters due to faulty or malicious devices, while as the volume and application space increases, these devices will be more prone to such cybersecurity attacks (imagine what an adversary could do with an access to a celebrity's medication device). If these medical end devices fail to work as advertised, at the least patients may lose trust using the devices and at the most, may endanger their lives. Therefore, it is very important to guarantee safety and security of those device. The proposed approach in this paper focuses on guarding such systems from safety failures due to cyber threats.

Safety Challenges. Existing methods of tracking medication adherence are far from being perfect and has many potential issues. Most commonly used pill count methods usually overestimate adherence[13]. Medication Event Monitoring Systems (MEMS)[14] suffer from several drawbacks. First, its cap is difficult to open with arthritic hands. Second, it does not report adherence in real time, so intervention cannot take place if medication time is missed. Third, it does not

---

[12] https://www.otsuka-us.com/discover/articles-1033
[13] https://www.affirmhealth.com/blog/pill-counts-a-tool-for-medication-adherence-and-diversion-reduction
[14] https://www.aardexgroup.com/solution/MEMS-adherence-software/22

accommodate the use of pill boxes for sorting medications into daily doses, as are commonly used by the elderly and when multiple drugs are taken. [6] discusses various causes of performance failures in infusion pumps[15]. These medical devices and solutions will be even more prone to failures due to network congestion and cyber attacks as they are increasingly getting connected to the internet.

Security Challenges. Cybersecurity threats (***CST***) are often indicative of weaknesses in the system design and those weaknesses make the system vulnerable to attacks by adversaries. As demonstrated[16], adversaries could forge an erratic signal with radio frequency electromagnetic waves in order to hack the implants inside the body. This false signal could inhibit required stimulation or induce unnecessary shocks in human brain and hence endanger life. This is just one example of medical device that can be hacked. Similarly, all MIoT solution can be hacked and threat vector becomes even larger when things are connected in order to push diagnosis and other data to cloud or health server. Therefore, it is paramount to design a structured approach and methods in order to do a comprehensive cybersecurity identification and analysis.

Mitigations. Actively looking for potential issues coming from different dimensions (such as SW defects or bugs, HW faults or failures, cyber attacks and human errors) and analyzing them on a continuous basis is very important, followed by identifying both static and dynamic mitigation strategies to ensure fault/attack tolerant operation of remote health monitoring solutions empowered by advanced communication technologies. Regulators, like the FDA, that approves such adherence monitoring products will also need to develop expertise in evaluating these safety and security issues in order to provide rigorous guidelines. The approach proposed below also considers countermeasures and provided some generic control methods in the use case part for certain type of common vulnerabilities in MIoT applications.

3   Approach

Here we propose a top-down, step-by-step approach to investigate and analyze cybersecurity threats and vulnerabilities of a medical device followed by control strategies to mitigate critical risks with higher impacts on safety of target patient. Essentially our approach has three stages viz., cybersecurity threat and vulnerability identification, risk assessment and risk control (See Figure 1).

3.1   Threat & Vulnerability Identification

The first stage should focus on identification of cybersecurity threats and vulnerabilities of the system under consideration. This can be done; first by formally

---

[15] https://www.fda.gov/medical-devices/general-hospital-devices-and-supplies/infusion-pumps

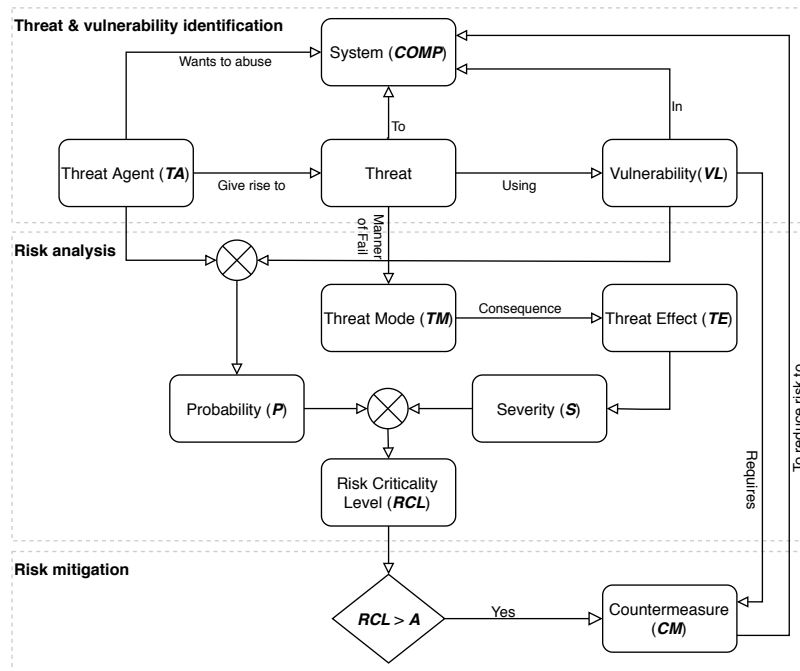[16] https://www.youtube.com/watch?v=FmFLAlZO6ig

Fig. 1. A step-by-step approach to investigate, analyze and mitigate cyber threats.

describing the different assets or components (**COMP**s) of the system. Threat agents (**TA**s) are people with bad intention and intend to exploit system vulnerabilities to damage the system under consideration. These **TA**s can be different based on the intention they have and all types should be identified. Following that random and intentional cyber threats that can endanger safety of a patient as well as all potential vulnerabilities (**VL**s) in the system should be identified. Both existing and emerging cyber threats should be envisage. Similar systems or products and their threat documentation can be referred to get more existing threats and internal and external information sources can be used to gain a better understanding of potential emerging threats.

3.2   Risk Analysis

The risk analysis is guided by the overall risk management process described in[17] (the flow chart is shown in figure 2 with minor modification to reflect the contribution of this paper). According to this standard; failure mode is defined as a manner in which an item fails and failure effect is defined as a consequence of a failure mode in terms of the operation, function or status of the item.

---

[17] ISO 14971: Medical device - Application of risk management to medical devices, 2012

A comparable cause-effect chain is suggested in [8] for security threat-effect as threat mode (TM) and threat effect (TE) and will be used same analogy in our approach as well. Therefore, TM is defined as manner of threat impact where as TE is defined as consequence of a TM in terms of the operation, function or status of the item and both should be identified in this stage.
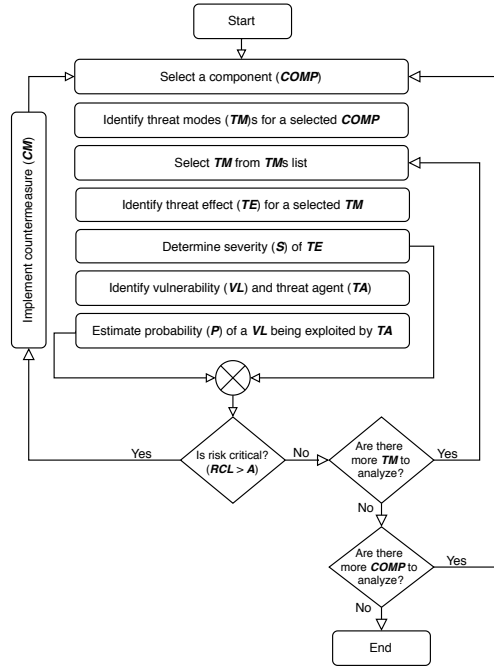

Fig. 2. Risk analysis process.

TE is quantified by defining severity (S) scale for a system under consideration and typical severity rates are indicated on a scale of 1 to 10 where 1 is lowest severity and 10 is highest. The chances of a VL being exploited is quantified by defining probability (P) scale and it depends on mainly vulnerabilities in a system but also target environment (EN) and the type of TA trying to damage the system. Risk criticality level (RCL) shows level of damage to a system caused by threat agent. This RCL can be determined based on the quantified severity and probability of occurrence. Eventual risk criticality level should be evaluated to know if the risk is minimal or significant. System specific S, P and RCL matrices should all be defined in this stage.

3.3   Risk Mitigation

In the third stage of our approach, countermeasures (CMs) will be suggested if risk criticality of a threat is not deemed to be acceptable. One or more of the

following risk **CM**s can be used in the priority order listed. The first one is to eliminate or reduce risks as far as possible (inherent safety by design), e.g. to add a safety mechanism. The second one is to take protective measures in the medical device itself or in the manufacturing process, e.g. an alarm, in relations to risks that cannot be eliminated as well as information of the residual risk due to any shortcomings of the protection measures adopted (though warning information is not considered as risk control measure, and not intended to lower any risk).

4   Use case

4.1   Intelligent Drug Dosing Device

OnDosis, here after called the Device, is a hand-held, digital and intelligent medicine container and dosing device to patients with chronic diseases such as attention deficit hyperactivity disorder (ADHD). It will transform existing systems into simpler and more convenient micro particles form integrated to an intelligent device. The Device prototype is shown in figure 3 where the display provides status information (e.g., dose size) and a disposable cartridge storing and dispensing a medicine formulated as granules. The device consists of a control unit programmed for a specific medicine and a disposable cartridge containing the specific medicine formulated as granules. The Device will comply in full with the standards[18] [19] [20] [21] [22] mandated by Radio Equipment Directive (RED).

Fig. 3. The OnDosis drug dosing device

---

[18] EN 55024 Information technology equipment - Immunity characteristics - Limits and methods of measurement

[19] EN 62479-2010: Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

[20] ETSI EN 301 489-1 ElectroMagnetic Compatibility (EMC) standard for radio equipment and services Part 1: Common technical requirements

[21] ETSI EN 301 489-17 ElectroMagnetic Compatibility (EMC) standard for radio equipment and services Part 17: Specific conditions for Broadband Data Transmission Systems

[22] ETSI EN 300 328 Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques;

4.2   Closed Loop Medication Management

All dispensing event(s) will be communicated to local monitoring unit (LMU), e.g., a smartphone over a Bluetooth low energy (BLE). Symptoms will be reported using LMU by the patient guided through questionnaires. Physical parameters will be recorded using smart wearable devices attached to a patient and will be communicated to LMU over Wi-Fi. These collected diagnostic data will be used for monitoring the patient condition on local premises using LMU and then will be pushed to cloud for remote monitoring. AI engine will be used for further automatic analysis and remote device setting and hence closed loop medication management (**CLMM**). Figure 4 shows the communication framework and data flows from the Device to LMU and then to cloud. OnDosis connectivity and synchronization of data from device to smartphone application through BLE connection.
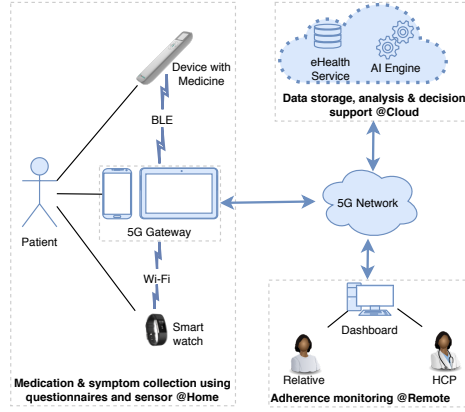

Fig. 4. OnDosis connectivity to LMU and Cloud.

Further connectivity to health server in order to provide decision support and remote adherence monitoring. This **CLMM** system will enable mobility, frequent & automatic data collection and local & remote adherence monitoring on a continuous basis.

4.3   Cybersecurity Analysis of the CLMM System

The approach explained in previous section will be applied in here to investigate cybersecurity related risks of the Device to improve its cyber attack defense to guard safety of patients.

Threat and Vulnerability Identification. Brainstorming sessions was performed with the device development team and identified the following details on device assets, usage environments, threat agents, threats and vulnerabilities.

On a higher level, the system comprises the dosing device, network technologies, local monitoring devices & services as well as cloud services as shown in figure 4. These different **COMP**s of the system are further listed in table 1 below.

The Device is intended for a Home Healthcare Environment in accordance with [23], but can also be used at school or office. The organization, production center and patient's home can be considered as indoor environments where the device will be connected to private network. Where as school, office and public gathering areas are considered as outdoor environments where the device will be connected to public network.

Table 1. Components

COMP-ID	Components
COMP-1	The Device
COMP-2	Software (SW) storage and SW execution in the Device
COMP-3	Configuration data, event data and device/SW parameters storage
COMP-4	Communications (in the device)
COMP-5	Communications (from device to LMU[1])
COMP-6	Communication (from LMU to edge/cloud services)
COMP-7	LMU and Diagnostic tools

[1] Local Monitoring Unit (e.g. Smartphone, Tablet, PC).

Threat agents can be grouped in different categories based on their intentions as well as target environment. For example, possible thereat agent at indoor environment is insider and intentions can be just curiosity to see certain undisclosed information. On another hand, hacker is a possible agent in outdoor environment and may have intention of harming a patient by altering system settings. Terrorists are agents with way bigger evil intention like mass destruction. Possible types of threat agents are shown in table 2, but only insider and hacker are considered as threat agent types for the use case system under study.

Table 2. Threat Agents

TA-ID	Threat Agents
TA-1	Insider
TA-2	Hacker
TA-3	Computer criminals
TA-4	Terrorists

Table 3 lists threat classes base on STRIDE model. Spoofing consists using someone else credential without their knowledge which usually targets weak authentications. Tampering is modifying a system or a data by adding or removing functional element and destroying or modifying data. Repudiating is

---

[23] IEC 60601-1-11 Medical electrical equipment — Part 1-11: General requirements for basic safety and essential performance

hiding attacker identity by erasing system logs or acting as some other by stealing credentials. Information disclosure involves data breaching to get a hold of confidential information. Denial of service is preventing user from accessing a system. Escalate privilege is acquiring additional privilege by spoofing user or tampering a system.

Table 3. Cybersecurity Threats

CST-ID	Cybersecurity Threats
CST-1	Spoofing
CST-2	Tampering
CST-3	Repudiation
CST-4	Information disclosure
CST-5	Denial of service
CST-6	Escalate privilege

TAs abuse a system by using **VL**s in it. For example if a system does not have user identification and authentication, then it is easy for an attacker to do unintended system settings which can result either system damage or death of a patient uses the system. Table 4 lists potential vulnerabilities in a medical devices.

Table 4. Potential Vulnerabilities

VL-ID	Vulnerabilities	Description
VL-1	Unverified SW	Poor software verification features
VL-2	Unprotected memory	Poor storage security features
VL-3	Interceptable network	Poor network security features
VL-4	Interruptable network	Poor interference rejection features
VL-5	Unauthorized connection	Poor entity connection verification
VL-6	No user identification	Poor device access authentication
VL-7	Weak user identification	Poor device access authentication
VL-8	Trojan circuit	Poor device electronics protection
VL-9	Weak malware defense	Poor malware protection
VL-10	Unverified data reception	Poor participant verification
VL-11	Unverified entity connection	Poor connection verification

Risk analysis. According to the approach; threat modes, threat effects, severity of effects, attack probability and risk criticality levels need to be determined in this stage. After surveying and collecting multiple potential threat related characteristics from literature and relevant standards, we zeroed-in on the following aspects based on critical thinking and discussions among development and verification teams.

A threat mode is a manner in which a system fail due to a cyber threat. Adherence monitoring on local device like smartphone will not be available if the BLE channel is continuously jammed. Hence, jamming the BLE network is a **TM**. Table 5 shows list of identified **TM**s for the **CLMM** system and their relation with specific threat type indicated in table 3.

Table 5. Threat Modes

TM-ID	Threat Modes	CST-ID
TM-1	Booting from a wrong boot SW	CST-3
TM-2	Executing a wrong SW	CST-3
TM-3	Unauthorized SW modification	CST-2
TM-4	Unauthorized data modification	CST-2
TM-5	Tampering HW	CST-2
TM-6	Injecting malware	CST-5
TM-7	Jamming network	CST-5
TM-8	Sniffing network	CST-4
TM-9	Tapping wired connections	CST-4
TM-10	Repudiating (acting as a genuine sender)	CST-3
TM-11	Unauthorized access to device features	CST-4
TM-12	Escalating access right	CST-6
TM-13	spoofing (disguise unauthorized changes)	CST-1
TM-14	spoofing (stealing credentials)	CST-1

Threat effect is a consequence of a certain threat mode. The consequence of jamming the BLE network is interruption of adherence monitoring service, hence the system is no longer available. One or more of the **TM**s shown in table 5 can result the **TE**s listed in table 6 and table 7 shows defined severity scales and their meanings (in the descending order of severity).

Table 6. Threat Effects

TE-ID	Threat Effects
TE-1	Inaccurate functionality
TE-2	Incorrect settings (dose size, time of medication)
TE-3	Incorrect diagnostic data
TE-4	Unable to use the device
TE-5	Wrong cartridge with wrong medicine
TE-6	Adherence service interruption
TE-7	Information disclosure
TE-8	Credential theft
TE-9	Drug abuse

The probability of a system being hacked by a hacker is higher in outdoor than indoor and therefore, target environments should be envisaged when esti-

Table 7. Severity

Level	Category	Description
4	Catastrophic	Patient death
3	Critical	Permanent impairment or life-threatening injury
2	Serious	Injury or impairment requiring professional intervention
1	Minor	Injury or impairment not requiring professional intervention
0	Negligible	Inconvenience or temporary discomfort

mating the probability of a vulnerability being exploited. The probability matrix for this system is defined in table 8.

Table 8. Probability of Occurrence

Level	Category	Description
4	Frequent	Likely to happen often
3	Probable	Likely to occur some times per year
2	Occasional	Can happen, but not frequently
1	Improbable	Unlikely to happen, rare, remote
0	Impossible	Will not happen

Table 9 shows defined risk criticality level (RCL) matrix which is derived by multiplying the quantified severity and probability of occurrence. If S is serious or below and the probability of occurrence is impossible or below, then the risk is considered as acceptable (A). Similarly, if P is improbable or below and the severity is minor and below, then the risk can be again considered as acceptable. Risks which are not insignificant but not clearly unacceptable are considered as elevated (L) risks. Risks in this region may be accepted if further risk is not practicable. Risks critical than elevated region are considered as unacceptable (U) risk.

Table 9. Risk Criticality Levels

		Probability				
		0	1	2	3	4
Severity	0	-	-	-	-	-
	1	-	A	A	L	U
	2	-	A	L	U	U
	3	-	L	U	U	U
	4	-	U	U	U	U

[A] Acceptable risk. [L] Elevated risk. [U] Unacceptable risk.

Risk mitigation. Vulnerabilities in a system requires countermeasure in order to reduce cyber related risks. If risk criticality is evaluated as acceptable, shown in green in table 10, then there is no need for implementation of any countermeasure as the threat impact on safety of a patient is minimal. However, if a threat mode give rise to elevated risk, marked in yellow in the table, or unacceptable risk, marked as red in the table, then the system requires countermeasure implementation to get rid of the corresponding vulnerability. The countermeasure column in the table provides suggestion on generic control mechanisms by leaving specific mechanisms, for example encryption type, for the system developer.

Table 10. Cybersecurity related risks and mitigation

TMs	TEs	S	VLs	TAs	P	RCL	CMs
The Device							
Unauthorized device access	Drug abuse	2	No user identification	Insider	3	U	User authentication
Unauthorized device access	Incorrect settings	4	No user identification	Insider	3	U	User authentication
Escalating privilege	Incorrect settings	4	Weak user identification	Insider	2	U	Force strong password
Software Storage and Execution in the Device							
Executing a wrong SW	Inaccurate functionality	3	Unverified SW execution	Insider	1	L	SW signature
Executing a wrong SW	Inaccurate functionality	3	Unverified SW execution	Hacker	2	U	SW signature
Unauthorized SW modification	Inaccurate functionality	3	Unprotected memory	Hacker	2	U	Memory protection
Configuration Data, Event data and Device/Software Parameters in Local Storage							
Unauthorized data modification	Incorrect settings	4	Unprotected memory	Insider	1	U	Memory protection
Unauthorized data modification	Incorrect settings	4	Unprotected memory	Hacker	2	U	Memory protection
Communications (in the device)							
Tapping wired connections	Information disclosure	1	Trojan circuit	Hacker	1	A	
Communications (from device to LMU)							
Spoofing	Incorrect diagnostic data	4	Interceptable network	Hacker	2	U	Encrypt data on transit
Sniffing network	Information disclosure	1	Interceptable network	Hacker	2	A	
Jamming network	Adherence service interruption	2	Interruptable network	Hacker	3	U	Frequency hopping
Repudiating	Incorrect diagnostic data	4	Unverified data reception	Hacker	2	U	User signature
Unauthorized entity connection	Incorrect settings	4	Unverified entity connection	Hacker	3	U	Entity authentication
Communications (from LMU to edge/cloud services)							
Spoofing	Incorrect diagnostic data	4	Interceptable network	Hacker	2	U	Encrypt data on transit
Sniffing network	Information disclosure	1	Interceptable network	Hacker	2	A	
Jamming network	Adherence service interruption	2	Interruptable network	Hacker	3	U	Frequency hopping
Repudiating	Incorrect diagnostic data	4	Unverified data reception	Hacker	2	U	User signature
Unauthorized entity connection	Incorrect settings	4	Unverified entity connection	Hacker	3	U	Entity authentication
LMU and Diagnostic tools							
Injecting malware	Unable to use the device	2	Weak malware defense	Hacker	3	U	Malware protection
Unauthorized SW modification	Inaccurate functionality	3	Unauthorized access	Hacker	3	U	User authentication

5   Concluding remarks

The result of the use case study demonstrates the impact of cyber threats on today's internet enabled monitoring and medication health solutions. Network and system integration security are important to consider in the product development and need to implement countermeasures for probable cyber related risks to guarantee safety of patients using such products.

A systematic approach is crucial for comprehensive identification of cyber threats and vulnerabilities of the system under consideration. Domain specific cybersecurity standards are prevalent and need to be commercially available to bind product developers to guarantee implementation of necessary countermeasures.

Investigating the security specification of existing advanced communication technologies would be beneficial, as a future work, to select technology with better security implementation and in such a way minimize the effort required from product developers.

Acknowledgements

References

1. Bedell, S.E., Jabbour, S., Goldberg, R., Glaser, H., Gobble, S., Young-Xu, Y., Graboys, T.B., Ravid, S.: Discrepancies in the Use of Medications: Their Extent and Predictors in an Outpatient Practice. Archives of Internal Medicine **160**(14), 2129–2134 (07 2000). https://doi.org/10.1001/archinte.160.14.2129
2. DiMatteo, M.R.: Variations in patients' adherence to medical recommendations: A quantitative review of 50 years of research. Medical Care **42**(3), 200–209 (2004), http://www.jstor.org/stable/4640729
3. Fotouhi, H., Causevic, A., Lundqvist, K., Björkman, M.: Communication and security in health monitoring systems - a review. In: COMPSAC 2016: The 40th IEEE Computer Society International Conference on Computers, Software & Applications (June 2016)
4. Hayes, T.L., Hunt, J.M., Adami, A., Kaye, J.A.: An electronic pillbox for continuous monitoring of medication adherence. In: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society. pp. 6400–6403 (2006)
5. Klugman, C.M., Dunn, L.B., Schwartz, J., Cohen, I.G.: The ethics of smart pills and self-acting devices: Autonomy, truth-telling, and trust at the dawn of digital medicine. The American Journal of Bioethics **18**(9), 38–47 (2018). https://doi.org/10.1080/15265161.2018.1498933
6. Paul, N., Kohno, T., Klonoff, D.C.: A review of the security of insulin pump infusion systems. Journal of Diabetes Science and Technology **5**(6), 1557–1562 (2011). https://doi.org/10.1177/193229681100500632
7. Rees, P., van der Gaag, N., de Beer, J., Heins, F.: European regional populations: Current trends, future pathways, and policy options. European Journal of Population / Revue européenne de Démographie **28** (2012), https://doi.org/10.1007/s10680-012-9268-z
8. Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E.: Security application of failure mode and effect analysis (FMEA). In: Bondavalli, A., Di Giandomenico, F. (eds.) Computer Safety, Reliability, and Security. pp. 310–325. Springer International Publishing (2014)
9. Ullah, S., Higgin, H., Siddiqui, M.A., Kwak, K.S.: A study of implanted and wearable body sensor networks. In: Nguyen, N.T., Jo, G.S., Howlett, R.J., Jain, L.C. (eds.) Agent and Multi-Agent Systems: Technologies and Applications. pp. 464–473. Springer Berlin Heidelberg (2008)