Attack-Tree based Risk Assessment on Cloud-oriented Wireless Body Area Network

Theodoros Mavroeidakos*, Nikolaos Tsolis*, Dimitrios D. Vergados* and Stavros Kotsopoulos§
*Department of Informatics, University of Piraeus, Piraeus, Greece
§Electrical and Computer Engineering Department, University of Patras, Patras, Greece
*{mavroeidakos,tsolis,vergados}@unipi.gr
,§kotsop@ece.upatras.gr

***Abstract*—Machine-to-Machine (M2M) communication is an emerging technology with unrivaled benefits in the fields of eHealth and mHealth. A significant subdomain of M2M communications is the Wireless Body Area Networks (WBANs), which exhibits high level of efficiency in collecting clinical health data. The WBANs coupled with the Cloud Computing (CC) paradigm introduce an ideal infrastructure in terms of performance and Quality of Services (QoS) for the development of eHealth applications. Nonetheless, due careful attention, the threats landscape in such a complex environment, is vast mainly due to the gathered data, which are sensitive. In this paper, a risk assessment aiming to avoid disclosure of Personally Identifiable Information (PII) and exploitation of software services, is introduced. The proposed assessment is based upon the implementation of a methodology. Initially, the health care WBAN-CC infrastructure is scrutinized; then, its threats' taxonomy is identified. Thence, the risk assessment is carried out based on an attack-tree consisting of the most hazardous threats against PII disclosure. Taken together the risk assessment and the threats' landscape, the implementation of several countermeasures is examined on account of effectively mitigating any gaps, which are indicated by the assessment.**

***Index Terms*—Risk Assessment, WBAN, CC, Threats Taxonomy**

I. Introduction

The health care domain consists of a cornerstone for the welfare of society. In the recent years there has been gaining much attention the convergence of emerging technologies such as the Big Data, the CC paradigm and the M2M communication architectural models. In the health care domain, sophisticated algorithms and novel processing techniques introduce benefits by minning Big Data and extracting knowledge while the CC paradigm establishes private back-end infrastructures, capable to handle massive quantities of clinical health data. The M2M architectural model, which is exploited in the health sector is comprised of mobile nodes, sensors and actuators interconnected to wireless networks through distributed base stations in the hospital's physical environment. Thus, a type of Wireless Sensor Networks (WSNs), the WBANs and their potential, unfold. The WBANs consist of a variety of on-body and implanted medical devices and sensors responsible for the continuous measurement of vital signs such as the temperature, the respiratory rate, the blood pressure and the arterial oxygen saturation.

The distributed nature of WBAN coupled with the fact that the data propagation by the sensors to backend systems of the M2M architecture, endanger the overall operation. By integrating CC backend endpoints, the already existing attack surface interacts with WBANs threats. These threats lie on the vulnerabilities of the M2M communications routing protocols and authentication schemes, as well as on spcific characteristics such as the swiftly changing network topology and unattended clinical areas. Thus, the threat landscape is expanded; therefore, the establishment of efficient risk assessment is crucial on the deployment of a cutting edge health care infrastructure.

The remainder of the paper is organized as follows. Section II introduces the background on securing critical infrastructures and assessing their security level such as those in health care while Section III outlines the architectural elements of WBAN-CC infrastructure apparatus. Section IV analyses the threats' taxonomy while Section V reviews the attack-tree upon which the risk assessment is implemented. Section VI contains the description of the risk assessment while examination of countermeasures is carried it out in section VII. The conclusions are drawn in Section VIII.

II. Related Work

In the literature there are few examples of security plans and methodologies aiming to protect the operation of infrastructures supporting eHealth and mHealth applications. Some preliminary work was carried out in the early 2006 by the European Commission (EU) on the subject of protecting critical infrastructures [1]. On the basis of this work, the back-end infrastructure supporting the provision of health care services is considered as critical due to the consequences that may emerge in case of an attack. In a cutting edge report of 2015 [2], the European Union Agency for Network and Information Security (ENISA) established a taxonomy of security challenges and risks that exist on the Information and Communications Technology (ICT) in the health sector of the Member-States of EU. Despite the fact that there is lack of harmonization with a unified strategy and specific roadmaps among the Member-States, the security requirements that should be fulfilled by the health care infrastructures, are identical. Over and beyond this, the cloud-based services in health care, as well as services processing Electronic Health Records (EHR) or Patient Health Records (PHR) should be treated as critical due to the security risk.

Furthermore, it has been suggested that the cyber and information security domain of hospitals should be reinforced with several precautions such as restricted access to intranets and confidential information, in order to mitigate threats [3]. Moreover, recent Strategic Note [4] of the European Political Strategy Center (EPSC), outlines that cyber-threats evolve quickly against critical infrastructures, which leads to the need of a European Cybersecurity Coordination Platform in order to enforce the Network and Information Security Directive ("NIS Directive") [5] of EU. According to [6], the National Institute of Standards and Technology (NIST), introduces a framework, which integrates risk management and cybersecurity activities into the operation of critical infrastructures so as to accomplish the desired outcomes in terms of data concealment. The framework is comprised of four Implementation Tiers that each one of them, form specific threat environment, legal and regulatory requirements, information sharing practices, business objectives and organizational constraints.

Our knowledge in securing critical infrastructures in essential societal sectors such as the Energy and the Environment, where large industries operate, is far more enriched than that on the sector of Health Care. The aim of our work is therefore to broaden the knowledge of protecting critical infrastructures on Health Care, comprised of WBANs and Cloud services. The proposed risk assessment encompasses the determination of threats by indicating the attack surface of the complex WBANs-CC environment; thence forward, the most hazardous attack sequences are analysed by virtue of an attack-tree coupled with the Multi-attribute Utility Theory [7].

III. Infrastructure Apparatus

A. WBAN-CC Infrastructure

Across the Health Care Infrastructure, the WBAN reinforces the clinical operation of the health care institution. The WBANs are comprised of nodes according the classification introduced by the IEEE Standard for Local and metropolitan area networks, 802.15.6 [8] [9]. Thus, the body area nodes are namely: implanted, body surface and external. The nodes' function is to monitor and log physiological parameters and vital signs such as non-invasive blood pressure and arterial oxygen saturation.

The concept of CC introduces unparalleled benefits not only concerning the economy but also on account of the hospitals' IT sector. In the case of the CC pardigm, the Cloud Service Provider (CSP) holds full responsibility about the operation and deployment of medical Software-as-a-Services (SaaSs). To this end, the hospitals' IT personnel is responsible about the designation of the SaaSs' requirements, the database scheme and the orchestration of the appropriate cloud-based services. On the other side, the CSP is accountable about certification issues related to the legislation but also to interoperability standards such as the Fast Health care interoperability Resources (FHIR). Over above this, the in the case of SaaS, the CSP is responsible about the security level of the back-end environment with respect to the legislation (i.e., General Data Protection Directive, NIS Directive) but also the security dependencies, which are extended by the signed SLA with each hospital.

B. Service Level Agreement

The Service Level Agreement (SLA) is consisted of Service Level Objectives (SLOs), which set the stage for the enforcement of specifications with regard to a high level of performance and security but also offer control over the restrictions of the CSP's operation. The SLOs focus on the the security of services and the data management. The enforcement of SLOs and the internal operations performed by the CSP will be audited by the hospital. The SLOs' enforcement is evaluated through metric units, which are defined by the hospital and are immediately associated with the goals of the SLA. These specific metric units also serve as a catalyst on understanding the CSP's performance according to what was previously agreed.

C. Cloud-centric mHealth Application

The state-of-art backend infrastructure supports the provision of a mHealth application that supports the operation of Personal Health Record (PHR). The PHR is assembled by a combination of SaaSs. Through the PHR, the management of schedules, review of patients profiles, lab results and examinations is enabled on the side of the hospitals medical staff (i.e. doctors, nursing staff). The body area nodes operation, facilitates the embodiment of additional capabilities to the PHR through a mHealth application which provides physiological data monitoring by aggregating measurements of specified vital signs with regard to the doctors consultation associated to the patients condition. To this end, the mHealth application's major attributes are the continuous remote monitoring of in-hospital patients, the optimal entanglement with harsh manifestations of diseases and adequate supervision of patients recovery from an acute event or surgical procedure.

IV. Threats Taxonomy

A. WBANs Threats

Overall, the incorporation of WBSNs or WBANs in the health care sector optimizes the quality of medical services and the treatment of patients, by performing swiftly Hematologic and Respiratory Measurements, but also collecting Bioelectrical Signals through the deployment of body area nodes. However, the gathering of clinical health data, introduces several privacy and ethics issues concerning the identity of individuals and their medical condition. These issues are highly associated not only to organizational objectives to the eHealth and pHealth sensors attack surface. Following the deployment of medical sensors such as the cardionet system [10], the aggregation of clinical health data is established in alignment with the clinicians' instructions. Having performed the measurements, the medical sensors dispatch the data to a SaaS for storing and further processing by using a short-range wireless network. However, in the course of this process, the Wireless BANs (WBANs) are threatened by the attacks [11] [12] [13], which are scrutinized on Table I.

TABLE I
WBAN THREATS CLASSIFICATION.

Layer	Attacks	Summary
Physical Layer	Jamming	This attack transmits malicious signals aiming to obstruct the communication of wireless nodes.
	Tampering	This attack modifies the parameters and credentials exchanged between the wireless nodes and the back-end infrastruSybilcture.
	Full Domination	This attack initiates exponential energy consuption in the MAC protocol and gathers information about the wireless network.
Data Link Layer	Selfish	This attack manipulates the wireless node's resources through vulnerabilities on MAC protocols.
	Intelligent Replay	In this attack the exploited wireless node replays SYNC packets to the other nodes in the same network.
	Collision	This attack injects malicious packets inside the WBAN aiming to damage the legitimate network traffic.
	Unfairness	This attack disrupts the MAC priority mechanism and distorts the network traffic.
	Denial of Sleep	This attack keeps the wireless nodes in an active state, extending the activities performed by them.
	Deauthentication	This attack sends deauthentication messages to wireless nodes and then captures the legitimate information used for authentication.
	Rogue Access Points (APs)	This attack lies on illegal activities of malicious devices placed side by side with the legitimate APs.
Network Layer	Selective Forwarding	In this attack malicious wireless nodes drop and selectively forwards packets causing damage to the network traffic's integrity.
	Sleep Deprivation	This attack aims at exhausting the power reserves of wireless nodes by keeping them busy with useless requests and activities.
	Sinkhole	In this attack a malicious wireless node derives the majority of network traffic via injection of false routing information.
	Sybil	This attack lies on exploiting the identity verification process of WBANs where the malicious node disguises its identity with multiple others.
	Wormhole	This attack discomposes the packets' propagation by deforming the routing information.
	Hello Flood	In this attack the malicious node lures the others into transmitting legitimate packets to it.
	Spoofing	In this attack the malicious node impersonates another as an intermediate stage to initiate other attacks or disclose information.
	Black Hole	In this attack the malicious node advertises false shortest paths to neighboring nodes as a means to disrupt the network traffic.
	Byzantine	This attack targets the routing protocol utilized by the nodes in the WBANs with scope to disrupt the data flow.
	ARP Poisoning	In this attack the malicious node reroutes the network traffic of others as a means to extract information and tamper with it.
	Resource Consumption	This attack degrades the network's latency and capacity by broadcasting Route Request (RREQ) packets.
Transport Layer	De-Synchronization	This attack desynchronizes the endpoints in an active channel between a wireless node and the AP by repeatedly sending fake messages.
	Flooding	In this attack the malicious node‘ establishes many connections in parallel with another node in order to exhaust its power reserves.
	DNS	This attack is coupled with malicious traffic monitoring and aims at hijacking the legitimate DNS requests and alter them.
	Fabrication	In this attack the malicious node injects false information and modifies the collected data.
	Sniffing	This attack can be used as the initial stage of a reconnaissance or on account of disclosing clinical health data collected by a node.
Session Layer	Session Hijacking	In this attack the malicious node masquerades as an end node of a session amongst nodes and intercepts valuable information.

B. Cloud Computing Threats

The CC environment is increasingly becoming a vital factor in the management and processing of big data such as clinical health data by introducing many benefits. In contradiction to this, the overlapping technologies operating cooperatively in CC, formulate the appropriate conditions for the generation of a wide spectrum of threats. A taxonomy of these threats is the presented on Table I.

V. Attack-Tree Assembly

The ultimate objective resides in the root node of the attack-tree indicating that the attacker has completed the penetration with success. In this paper, given the analyzed health care infrastructure, this objective is the disclosure of Personally Identifiable Information (PII) such as demographics, sensorial data and clinical health data. Having identified the objective with the worst impact on account of both the treated individuals and the health care institution, the designation of the secondary objectives in the child nodes leading to disclosure of PII, is carried out.

The events that lead to a secondary objective are separated amongst them with OR and AND logical gates. Events that result to the secondary objectives and which are associated with AND-gates are treated by the attacker as coupled events. In the case of coupled events, the attacker is required to accomplish them all in order to proceed. In the case where OR-gates reside, the attacker deals with them as isolated events. As a result, the occurrence of an isolated event leads directly to the secondary objective. The examined attack-tree can be extended by acknowledging further penetration scenarios. Having assembled the attack-tree illustated in Fig. 2, thereupon the four attribute values presented on Table 2, are assigned to each node. The immediately preceded nodes by the root causing disclosure of PII are notated by M_{11}, M_{12}, M_{13}, M_{14} and M_{15}, denoting *Eavesdropping Wireless Traffic*, *Break in the Wireless Network*, *Gain Administrative Back-end Access*, *Connection to Cloud API* and *Data Warehouse Discovery* respectively. Given the fact that the attacker has reached any of the root's child nodes, disclosure of PII is achieved in different layers of the health care infrastructure.

A. Attack Sequences Analysis

On the grounds of demonstrating the penetration sequences favored in the assembled attack-tree, a thorough analysis of several attacks is carried out.

The objective M_{11}, *Eavesdropping Wireless Traffic* is accomplished with two approaches, either by reaching the objective, M_{111}, *Capture Wireless Traffic* and apply *Network Traffic Analysis* or by implementing the remaining AND-gate events. The objective, M_{111}, *Capture Wireless Traffic* can be achieved by following three paths.

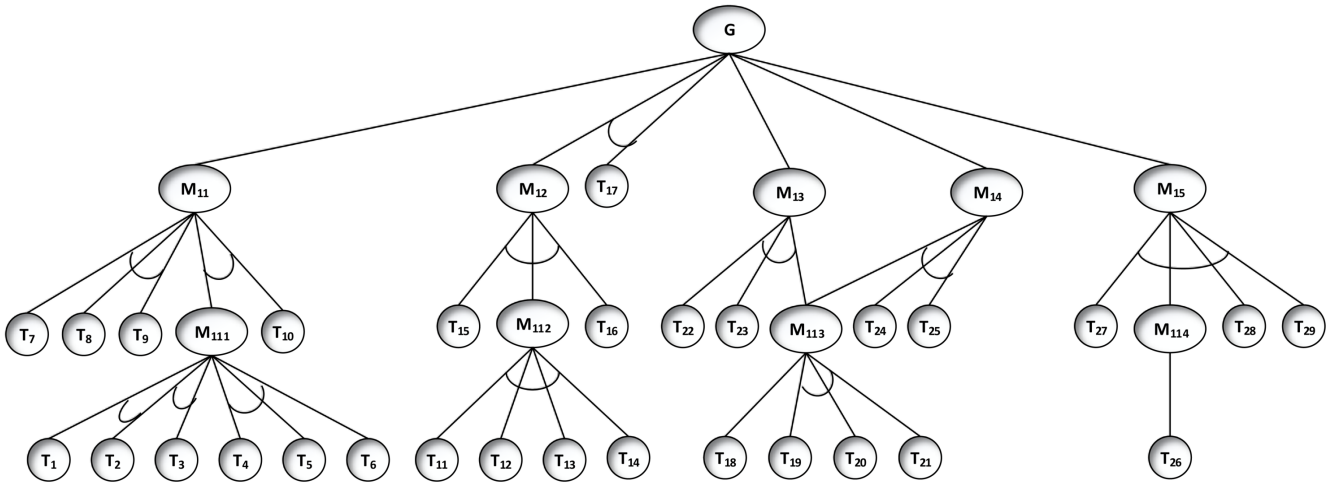
- By acquiring access to the hospital's unauthorized areas such as the internal physical environment of Intensive Care Unit (ICU), the attacker is in position to emplace malicious sensor nodes. In this environment, by cause of the patients' harsh physiological conditions, multiple medical sensors are attached to the individuals with scope to gather clinical health data.
- Beyond the injection of malicious sensors inside unauthorized areas, the attacker is able to further tamper with the already attached medical sensors in order to upload a revised version of their software wherefore he acquire access to the gathered data.
- Over and above the previous approaches, having exploited a router by testing recursively username - password combinations or bugs such as the Shellshock, the attacker injects a malware in the router, which thereupon enables him to gain command and control over the ongoing spectrum of operations. In this approach, the attacker should cover his track in order to maintain long-term unauthorized access to the exploited router.

The AND-gate events leading to M_{11}, illustrate the novel Key Reinstallation Attack (KRACK) [14], which exposes Wi-Fi networks protected by Wi-Fi Protected Access 2 (WPA2) standard encryption and decrypts the victim's network traffic. The KRACK targets the 4-way handshake providing mutual authentication and session key agreement between the Access Point (AP) and the cients. The vulnerability upon which the KRACK is based, is the fact that the (AP) will re-transmit message 3 of the 4-way handshake, which is responsible about the key installation on the client side, multiple times given that an acknowledgment is not received. Each time that the client receives the key, it will reinstall the same session key, and subsequently the *incremental transmit packet number* (nonce) and the *receive packet number* (i.e., replay counter) are reset to their initial value. This event enables on the attacker, the capability to collect and replay re-transmissions of message 3 in order to force nonce resets. The AND-gate events composing the KRACK, are summarized as:

- Deploy rogue access point in order to manipulate 4-way handshake messages.
- Enable network traffic forwarding.
- Initiate the KRACK malicious script.

The objective M_{112}, *Capture Wireless Traffic with Encrypted Format of Password* is realized with a distinct process. In this attack, the perpetrator attempts to breach the enterprise Wi-Fi network providing access to the hospital's staff and connect to it. The majority of these networks are usually protected only with the WPA2 standard encryption. The only limitation that emerges, is that the attacker should be within the wireless coverage of the AP. The same limitation applies also in the approach with tha KRACK. by acquiring access, the perpetrator targets web interfaces where the nursing staff registers the demographics. Therefore, through fields in the web forms, the perpetrator may initiate application layer attacks such as SQL injection. The events leading to the M_{112}, are classified as:

- Choose an AP by its channel and then proceed with information gathering concerning its operation such as clients' enumeration.



G	Disclosure of Personally Identifiable Information (PII)
M_{11}	Eavesdropping Wireless Traffic
M_{12}	Break in the Wireless Network
M_{13}	Gain Administrative Backend Access
M_{14}	Connection to Cloud API
M_{15}	Data Warehouse Discovery
M_{111}	Capture Wireless Traffic
M_{112}	Capture Wireless Traffic with Encrypted Format of Password
M_{113}	Gain Access to Server
M_{114}	Connection to Compromised Machine
T_1	Malicious Sensor Node Injection
T_2	Acquire Access to Unauthorized Areas of Hospital
T_3	Medical Sensor Tampering
T_4	Infect a Router with Malware
T_5	Gain Command & Control
T_6	Conceal malicious connection behind a proxy chain
T_7	Deploy Rogue Access Point
T_8	Enable Traffic Forwarding
T_9	Execute KRACK malicious script
T_{10}	Network Traffic Analysis
T_{11}	Enumerate Client Devices
T_{12}	Target one of the Hospital's Access Points by its Channel
T_{13}	De-Authenticate Client Devices
T_{14}	Capture four-way Handshakes during Automated Authentication
T_{15}	Create a Profiled Dictionary
T_{16}	Brute Force the Wireless Traffic File
T_{17}	Deploy Monitoring Equipment/Services
T_{18}	Social Engineering
T_{19}	Information Gathering
T_{20}	Services Enumeration
T_{21}	Vulnerability Identification/Exploitation
T_{22}	Privileges Escalation
T_{23}	Data Repository Reconnaissance
T_{24}	Enumeration of Associated Cloud APIs
T_{25}	Information Gathering of Unsecured Cloud APIs
T_{26}	Client Side Attack on Personnel
T_{27}	Network Foot printing
T_{28}	Restful Cloud APIs Enumeration
T_{29}	HTTP Parameter/Path Pollution Attack to add Attacker on Administrative Group

Fig. 1. Attack-tree of WBAN-CC infrastructure.

- Enumerate the client devices, such as terminals where the nursing staff registers demographics but also personal computers, which are utilized by doctors in order to access PII.
- De-authenticate client devices forcing them to automatically initiate the re-authentication procedure with the AP.
- Capture the 4-way handshakes between the clients and the AP.

Then, having gathered network traffic with 4-way handshakes, the perpetrator can brute force it with a custom dictionary formed by the hospital's web footprint and characteristics, such as the type of clinics and its medical specialization (i.e., orthopedic incidents, oncological). The result of a succesful attack of this type, is that the perpetrator puts the password that authorizes access in the wireless network in his position. Overall, following the initial stages of any attack (e.g. passive and active information gathering), the attackers are in position to coordinate their penetration technique by combining vulnerabilities both in the whole infrastructure. To this end, new attack vectors emerge due to the conjunction of these technologies and as a result the threats impact on the end-service, is hazardous.eless network in his possession.

The objective M_{113}, *Gain Access to Server* consists of the most hazardous attack. In this attack, the perpetrator targets the back-end servers supporting the hospital's operations such as patients' registration and logging of clinical health data. On account of accomplishing this attack, either the three AND-gate events or social engineering should be carried out. The aim of social engineering is to exploit vulnerabilities lying on hospital's staff behavioral patterns. Social engineering is one of the most efficient approaches to breach security due to the fact that exploits the human factor interacting with the systems of interest. The AND-gate events are broken down into the following:

- Information Gathering.
- Services Enumeration.
- Vulnerability Identification & Exploitation.

The M_{113} coupled with post exploitation events such as the

TABLE II
STANDARD ATTRIBUTE VALUES.

Attack cost	Technical difficulty	Probability to be discovered	Probability to be utilized	Degree
>1	quite difficult	quite simple	very high	5
0.8 - 1	difficult	simple	high	4
0.5 - 0.8	mediate	mediate	moderate	3
0.2 - 0.5	simple	difficult	low	2
<0.2	quite simple	quite difficult	very low	1

Privileges Escalation and *Data Repository Reconnaissance* leads to the ultimate objective, M_{13}. On the other side, this objective can be used as the intermediate stage to a cloud attack; hence this objective may be combined with events such as *Enumeration of Associated CLoud APIs* and *Information Gathering* in order to achieve the objective, M_{14}.

The objective M_{114}, *Connection to Compromised Machine* exists in the health care infrastructure by cause of client side attacks on the hospital's personnel. The client side attacks contain interception of user sessions, cross-site scripting, insert malicious content, conduct phishing attacks and acquire cookies. These techniques enable on the perpetrators side, complete control over the client's browser and thence oversight over the managed PII. The M_{114} conjoined with the events *Network Foot Printing*, *Restful Cloud APIs Enumeration* and *HTTP Parameter/Path Pollution Attack* in order to add the attacker's identity on the Administrative Group, lead to the objective M_{15}.

VI. RISK ASSESSMENT

Across the health care infrastructure, throughout the communication paths between the edge interfaces and the back-end assets, reside the most valuable resources, PII and the patients' clinical health data. With the prospect of disclosing clinical health data, the attacker has to take into consideration both the edge points of the health care infrastructure, which can be approached and where vulnerabilities may exist but also the encountered risk regarding his exposure. As a result, four attributes are assigned to each leaf node in order to conclude in what degree, the attacks are accomplishable. These demonstrated attributes on Table 2 are namely, the *Attack Cost*, the *Technical Difficulty*, the *Probability to be discovered* and the *Probability to be utilized*, which are denoted as c_T, d_T, s_T and t_T, respectively. The assignment of attributes to the leaf nodes is performed empirically, based upon the experience of the security expert of the WBAN-CC infrastructure.

The security expert is burden with the legal obligations instructed by the General Data Protection Regulation (GDPR) [15] beyond the security responsibility concerning the health care infrastructure assigned by the institution. Thus, he or she operates with the role of a Data Protection Officer (DPO) inside the hospital, enforcing compliance of the legal instructions practically. The risk assessment serves as a complementary part of the *Data Protection Impact Assessment*, which is a mandatory part in the context of ensuring compliance with GDPR in order to prove that processing operations are safeguarded by the appropriate technical and organizational measures. In this high risk infrastructure, the security expert assigns values to the attack-tree's leaf nodes by taking into consideration several factors such as the level of the attacker's experience and knowledge set, the number of cooperating attackers, the attacker's purpose, the specialization of wireless equipment and tools, as well as the attacker's profit given that the attack-tree's root node is achieved. The assigned attribute values to the leaf nodes are demonstrated on Table 3. The the Multi-attribute Utility Theory is utilized to transfer the four attributes into the attacker's utility value P_T. The utility value, P_T, indicates the occurrence probability of each leaf node, which is calculated by the following formula (1) and presented on Table 3:

$$P_T = W_c \times U_1(c_T) + W_d \times U_2(d_T) + W_s \times U_3(s_T) + W_t \times U_4(t_T) \quad (1)$$

The occurrence probability depends on a number of weighting coefficients, which are adjusted by the security expert according the system's deployment and his experience in the operation of defensive mechanisms. These coefficients are set to the following values, $W_c = \frac{1}{3}$, $W_d = \frac{1}{4}$, $W_s = \frac{1}{4}$ and $W_t = \frac{1}{6}$, where their sum is, W_c+W_d+W_s+W_t=1. The $U_i(x)$ consist of the utility function of each attribute and its value is, $U_i(x) = \frac{c}{x}$ where $i \in \{1, 2, 3, 4\}$. The normalization factor c is assigned to the value, 0.4.

Following the attack sequences' assessment and the overall occurrence probability that each one demonstrates, the security expert is able to efficiently address security gaps, which endanger PII. To this end, the risk is estimated by the formula (2) as the product of the occurrence probability of root node, G and damage, which may be classified to three categories with regards to the amount and the type of disclosed PII namely, *Low*, *Medium* and *High*. In the *damage* category, the following values, 900, 1000 and 1100, are assigned respectively. The Cost corresponds to the expenses that the security equipment bears.

$$Risk = \frac{Occurrence\ probability\ of\ G \times Damage}{Cost} \quad (2)$$

VII. EVALUATION

The described risk assessment can be integrated in a security model such as the one which, is showcased in Fig.2 in order to optimally engage in the WBAN-CC infrastructure.

TABLE III
VALUES ASSIGNED TO THE ATTACK-TREE'S LEAF NODES.

Leaf Node	c_T	d_T	s_T	t_T	P_T
T_1	5	4	5	2	0.083
T_2	4	3	3	3	0.122
T_3	5	5	1	3	0.169
T_4	4	4	2	4	0.125
T_5	4	3	4	5	0.105
T_6	2	2	3	5	0.163
T_7	4	2	4	5	0.122
T_8	2	1	1	5	0.280
T_9	5	2	2	5	0.140
T_{10}	4	3	1	5	0.180
T_{11}	3	2	3	5	0.141
T_{12}	4	3	2	4	0.133
T_{13}	4	1	2	5	0.197
T_{14}	5	2	2	4	0.143
T_{15}	2	4	1	4	0.208
T_{16}	3	2	1	4	0.211
T_{17}	5	4	3	4	0.102
T_{18}	5	5	2	4	0.113
T_{19}	3	2	4	5	0.133
T_{20}	3	3	4	5	0.116
T_{21}	5	5	4	5	0.085
T_{22}	4	3	2	4	0.133
T_{23}	4	3	3	4	0.117
T_{24}	4	4	3	5	0.105
T_{25}	4	4	4	5	0.097
T_{26}	3	3	2	4	0.144
T_{27}	4	2	4	5	0.105
T_{28}	4	4	4	4	0.100
T_{29}	5	4	3	3	0.107

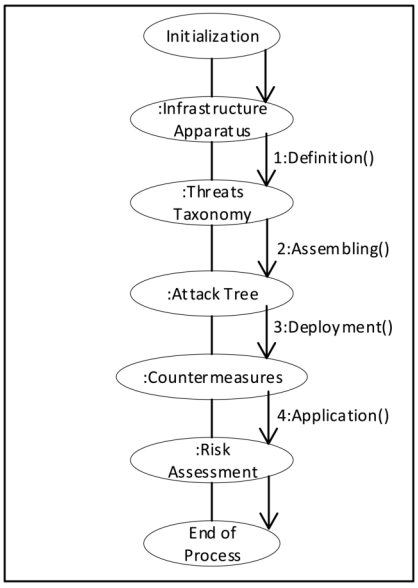


Fig. 2. Security model employing attack-tree based risk assessment.

The presented security model consists of five distinct layers through which the security objectives are fulfilled across the health care infrastructure. These layers are tailored to mitigate threats against professional opponents targeting the advanced cyber-physical components composing the infrastructure.

A. Countermeasures

The WBANs should be deployed according to the security measures of IEEE 802.15.4 standard. Moreover, with regard to the standard IEEE 802.15.6 [16], the wireless networks should operate by following a security level in order to provide in turn specific security mechanisms. These levels are namely, the Level 0, in which unsecured communication takes place, the Level 1, in which the authentication is of great importance but there is no encryption and the Level 2, which supports strong authentication as well as encryption.

Having deployed the medical sensors in an ad-hoc based architecture, the mesh construction of APs is costly to be supported by Wireless Intrusion Detection System's (WIDS) sensors. Furthermore, in case that the WIDS has embedded a prevention feature then multiple medical sensors or even PSs transmiting medical data, can be derived from the network due to false positives. This security measure poses certain performance and quality of service limitations. In order to overcome these limitations, the ISO/IEC/IEEE P21451-1-4 standard could be employed. Over and above that, the WBAN countermeasures are summarized on Table 1.

Due to the management of the cyber-infrastructure's many aspect, compatibility issues concerning the TLS protocol are nonexistent. Appropriately, the TLS version 1.2 is to be configured as the default in every endpoint residing in public and management network and the TLS versions 1.0, 1.1 and every version of SSL are to be disabled entirely. In the event that the configuration of TLS version should be guided by the *RFC 7507* and therefore supported by the extension *TLS_FALLBACK_SCSV* in order to abstain fallbacks from higher to lower versions or protocols. Another key consideration is that the encryption's strength used in TLS sessions, depends on the cipher, which is settled between the endpoints. Hence, a strong ciphersuite should be selected and the usage of sufficiently large key sizes should be incorporated during the configuration process. Beyond these practices, TLS renegotiations should be established in compliance to the *RFC 5746*. Ciphers and protocols, which are not adequately secure have to be deactivated.

VIII. CONCLUSIONS

The proposed risk assessment aims at achieving a high level of security and privacy inside a health care infrastructure, through the analysis of attack sequences based on an attack-tree. The risk assessment serves as ensurance on account of the security level and the level of cohesion amongst the countermeasures. Through the assessment, considerable insight has been gained with regard to the vulnerabilities and points of interest, which should be taken into consideration in the protection of the patients' PII. The results indicate

TABLE IV
SPECTRUM OF COUNTERMEASURES MITIGATING THE ATTACKS SURFACE.

Field	Countermeasure	Summary
WBANs	IEEE 802.15.6 standard [16]	The WBANs should operate by following a security level (i.e., Level 0, Level 1, Level 2) in order to provide in turn specific security mechanisms ad secure the communication.
WBANs	Biometrics scheme in cryptographic operations [9] [17]	Manipulation of physiological signals (i.e., ECG), with the scope to be utilized as inputs to pseudo-random generators. These methods enforce the process of encrypting and decrupting keys, which are involved in the Tier-1 communication.
WBANs	Wireless Intrusion Detection System [18]	The network traffic propagated amongst the entities of Tier-1, is collected by Kismet drones and monitored by a daemon running over the Kismet server.
WBANs	ZigBee security controls [19]	The security controls of ZigBee extend the countermeasures established on IEEE 802.15.4 standard concerning authentication and encryption keys distribution.
WBANs	Wireless Security Protocols [19]	Usage of protocols such as WiFi Protected Access (WPA) and WiFi Protected Access version 2 (WPA-2).
WBANs-CC	Encryption techniques [19]	Symmetric key encryption, Conventional Public Key Encryption, Identity Based Encryption, Elliptic curve cryptography and Attribute-based Encryption.
WBANs	Secure Routing	Usage of protocols such as Ariadne, Secure Efficient Ad-hoc Distance vector (SEAD) and the Authenticated Routing for Ad Hoc Network (ARAN).
WBANs	ISO/IEC/IEEE P21451-1-4 standard	The orchestration of this standard facilitates intrusion prevention by employing the eXtensible Messaging and Presence Protocol (XMPP), which enables Deep Packet Presence Protocol (XMPP), which enables Deep Packet Inspection (DPI) in the lower levels of network packets.
WBANs	802.11 Secure Configuration	APs signal strength calibration, auto-connect feature of PSs for connection with APs should be used with caution, enabling APs' security controls, disabling default credentials.
WBANs	Data Layer Defenses [20]	Error correction code, small frames, rate limitation.
WBANs	Network Layer Defenses [20]	Encryption, egress filtering, authorization monitoring
WBANs	Transport Layer Defenses [20]	Client Puzzles, Authentication
WBANs-CC	Transport Layer Security (TLS) protocol version 1.2	Implementation amongst endpoints in ICU(i.e., WBANs and mHealth application) and CC.
WBANs-CC	TLS Secure Deployment	RFC 7507 (i.e., flag *TLS_FALLBACK_SCSV*), selection of strong ciphersuite, orchestartion of large key sizes, TLS renegotiations in compliance with RFC 5746.
CC	STaaS Secure Configuration	Executed under a non-root service account, Alteration of default listening ports, orchestration of API key tokens for authentication, employment of private Virtual Local Area Network (VLAN) between load balancer and proxies.

which components should be reinforced with countermeasures as means to achieve end-to-end control and governance. This paper broadens the set of knowledge in protecting critical infrastructures on Health Care, comprised of WBANs and CC environment by implementing attack-tree based risk assessment.

ACKNOWLEDGMENT

The publication of this paper has been partly supported by the University of Piraeus Research Center (UPRC).

REFERENCES

[1] European Commission (EU). "COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection". 2006. [online] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33260.

[2] European Union Agency For Network And Information Security(ENISA). "Security and Resilience in eHealth, Security Challenges and Risks". 2015. [Online]. Available: https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services.

[3] A. Djalali and P. Ingrassia, "Best practices of health sector and EU hospitals for risk management and reduction against terrorist attacks and inter-organisational plans". 2016. [online] Available at: http://www.threatsproject.eu/work.html.

[4] European Commission, European Political Strategy Center (EPSC) Strategic Notes. "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level". Issue 24, 2017. [Online]. Available:https://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en.

[5] NIS Directive: officially Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[6] National Institute of Standards and Technology (NIST). "Framework for Improving Critical Infrastructure Cybersecurity". Draft Version 1.1. 2017. [Online]. Available: https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.

[7] Sarin R.K., "Multi-attribute Utility Theory," in: Gass S.I., Fu M.C. (eds) Encyclopedia of Operations Research and Management Science. Springer, Boston, MA, 2013.

[8] Institute of Electrical and Electronics Engineers (IEEE), IEEE Standard for Local and metropolitan area networks-Part 15.6: Wireless Body Area Networks, 151-172, https://standards.ieee.org/findstds/standard/802.15.6-2012.html Accessed 15 January 2017.

[9] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith and A. Jamalipour, "Wireless Body Area Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1658-1686, Third Quarter 2014.

[10] P. Kakria, N. K. Tripathi, and P. Kitipawang, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors". Int. J. Telemedicine Appl. 2015, Article 8, January 2015.

[11] S. Saleem, S. Ullah, and K.S. Kwak, ”A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks”. Sensors, 11(2), pp. 1383-1395, 2011.
[12] Khan S. and Pathan A.-S. K., ”Wireless Networks and Security: Issues, Challenges and Research Trends”. 170-191, Springer, 2013.
[13] Jo M., Han L., Tan N. D. and In H. P., ”A survey: energy exhausting attacks in MAC protocols in WBANs,” in Telecommunications Systems, 58, 153-164, 2015.
[14] Vanhoef, M. and Piessens, F., ”Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” in Proceedings of the ACM Conference on Computer and Communications Security, Dallas, TX, USA (Vol. 30), 2017.
[15] General Data Protection Regulation: officially Regulation 2016/679 on the protection of natural persons in regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [online] Available at: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679.
[16] Institute of Electrical and Electronics Engineers (IEEE). Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks. IEEE Std 802.15.6-2012, pages 1271, 2012.
[17] Farrukh Aslam Khan, Aftab Ali, Haider Abbas, and Nur Al Hasan Haldar. A cloud-based healthcare framework for security and patients data privacy using wireless body area networks. Procedia Computer Science, 34(Supplement C):511517, 2014.
[18] Jason Murray and R Wanner. An inexpensive wireless ids using kismet and openwrt. SANS Institute, pages 89, 2009.
[19] Samaher Al-Janabi, Ibrahim Al-Shourbaji, Mohammad Shojafar, and Shahaboddin Shamshirband. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 2016.
[20] Shafiullah Khan and A. Khan Pathan. Wireless networks and security. Springer, Berlin, 1 edition, 2013.