Security threats against the transmission chain of a medical health monitoring system

Juha Partala*, Niina Keränen†, Mariella Särestöniemi‡, Matti Hämäläinen‡, Jari Iinatti‡,
Timo Jämsä†, Jarmo Reponen§ and Tapio Seppänen*
* Department of Computer Science and Engineering
University of Oulu, Finland
Email: givenname.surname@ee.oulu.fi
† Department of Medical Technology, University of Oulu, Finland
Email: N. Keränen givenname.surname@fimnet.fi, T. Jämsä givenname.surname@oulu.fi
‡ Centre for Wireless Communications, University of Oulu, Finland
Email: givenname.surname@ee.oulu.fi
§ FinnTelemedicum, University of Oulu, Finland and Raahe Hospital, Raahe, Finland
Email: givenname.surname@oulu.fi

***Abstract*—One of the most important aspects of a wireless health monitoring system is the security of data. In this paper, security attacks against the complete transmission chain of a medical health monitoring system are enumerated and classified based on their threat to three security principles: confidentiality, integrity and availability. The communication chain is divided in a standard way into three tiers and relevant threats are identified for each tier. Security requirements corresponding to these threats are presented. It is noted that end-to-end security is not feasible due to distributed computing and the incompatibility of the data standards of different tiers.**

***Keywords*—Body sensor networks, Health information management, Communication system security, Information security**

I. Introduction

Developments in telemedicine, personal health, and ubiquitous sensors are expected to improve both the quality and cost-effectiveness of healthcare. These advances are sorely needed to help healthcare systems cope with the challenges brought on by an aging population and increasing chronic illness. As the wireless communications in remote monitoring and worn actuators increase, so do new kinds of security risks [1]–[3] and vulnerabilities. Strict ethical and legal requirements are placed on the confidentiality and security of medical data for the entire length of the communication chain [4].

A wireless health monitoring system typically consists of the following components. There are one or multiple wireless sensors organized into a wireless body area network (WBAN). Such a network communicates with a central hub that transfers data to an end server through a gateway device such as a smartphone. The end server typically resides on a wired network. For example, CodeBlue [5] and Alarm-net [6] are research projects based on such a configuration. Such systems can be used, for example, to detect seizures [7]–[9] or to monitor neuromotor conditions [10]–[13].

The threat model for the data flow in a wireless health monitoring system is not easy to formulate. Due to the number of different communication networks on the transmission chain, there is a diversity of security threats that apply to different parts of the chain. In this paper, the aim is to concisely enumerate known threats upon the complete transmission chain ranging from threats against WBAN to threats against the end server. Since there are various subcomponents, the communication of the chain is considered using a standard 3-tiered structure [14], [15] based on the proximity of the communication to a patient. Relevant threats to each tier are identified based on the properties of the tiers. Transfer of data from a tier to the next is also considered.

There are publications discussing security threats against health monitoring systems in general [16] as well publications concentrating on various subcomponents of the transmission chain such as wireless sensor networks [17], [18]. There are also publications concentrating on specific security goals such as the privacy of a patient [19]. However, threat analysis concentrating on the security for the complete transmission chain and identification of relevant threats at each point of the chain have not been considered before.

There are various ways to classify different attacks to a network. In [20], attacks are classified into outsider and insider attacks depending on whether the attacker is part of the network. In this paper, attacks are divided by the threat they pose to three key security principles: *confidentiality*, *integrity* and *availability* (the CIA model). Another useful way is to divide the attacks into two sets based on the activity of the adversary. *Passive attacks* are those attacks that do not require the adversary to actively transmit messages into the network. Such threats can be hard to notice, since no traces are left by the adversary. In an *active attack*, the adversary actively tries to bypass the system either by injecting messages into the network or by other means.

The paper is organized as follows. Section II briefly describes a typical health monitoring system and the transmission chain from the patient to the end server. Section III reviews the attacks found in the scientific literature that can lead to a violation of one of the three security principles. In Section IV, relevant threats and the corresponding security requirements are identified for each tier. Finally, Section V concludes the paper.

978-1-4673-5800-2/13/$26.00 ©2013 IEEE

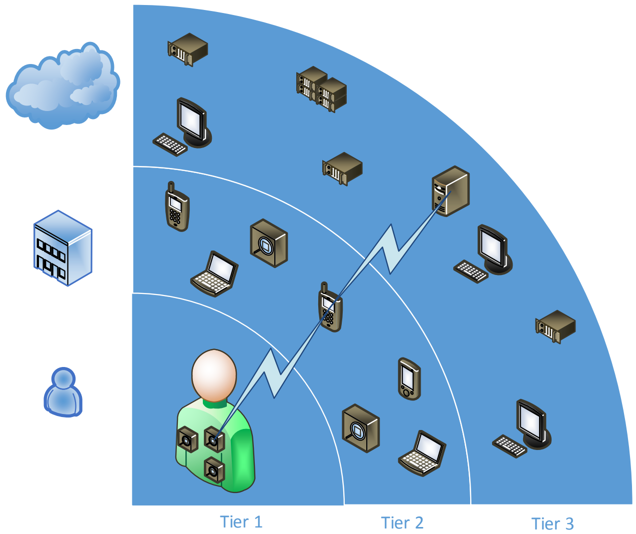

Fig. 1. The communication tiers

II. The Transmission Chain

A typical wireless health monitoring system [6] is considered. The system consists of wearable wireless medical sensors organized into a WBAN. It is assumed that the WBAN is organized into star or tree topology [21], [22] and outside communication is routed through a central hub. The central hub communicates with a gateway device such as a smartphone using for example Bluetooth or ZigBee. There may also be external environmental sensors communicating with the gateway device [6]. The gateway device functions as an access point to the end server that resides on a wired network such as Internet.

The communication of the system is divided into 3 tiers [14], [15]. Tier 1 consists of intra-WBAN communication between the nodes and the central hub. It has a limited radio range of approximately 5 meters. The second tier consists of communication between the gateway device and the central hub as well as communication among external sensors and other devices able to communicate with the gateway device. Tier 2 has a greater radio range of up to 100 meters (for example Bluetooth class 1) and comprises a variety of different devices with varying capabilities. Tier 3 consists of the rest of the transmission chain from the gateway device to the end server over a public network such as Internet. The general setup is depicted in Fig. 1.

III. Attacks

In this section, attacks against wireless health monitoring systems are enumerated.

A. General attacks

Attacks that can compromise all of the three security principles have been classified as general attacks. These attacks are arguably the most severe and have consequently also been the most successful ones. General attacks have been listed in Table I.

TABLE I. General attacks

Attack	Description	Active(A)/ Passive(P)
Hardware compromise	Tampering a node or another part of the system.	A
Software compromise	Exploitation of a software vulnerability.	A/P
Subversion	Introduce a hidden hardware or software backdoor into the system. Can be hard to notice.	A
Malware	Using for example viruses and worms.	A
Social engineering	Gaining access to the system by fooling either the patient or someone with legitimate access to the information.	A
Man-in-the-middle	The attacker makes connections between the end points and relays messages between them. The communication is completely controlled by the attacker.	A

TABLE II. Attacks against confidentiality

Attack	Description	Active(A)/ Passive(P)
Eavesdropping	Listening to radio communication or inspection of packets on route.	P
Location tracking	Locating the patient based on radio signals or other information provided by the system.	P
Condition tracking	Tracking patient condition. If the system is scheduled, for example, to transmit only on changes to the condition of the patient, these changes can be tracked by outsiders.	P
Patient impersonation	Falsely claiming to be the patient to assume control of the system and to obtain private information.	A
Node impersonation	Impersonation of a node in the network using for example replication [24].	A
Side channel attacks	Taking advantage of properties of the physical implementation of the system such as timing information to accrue sensitive information. Can be also applied actively.	A/P
Traffic analysis	Inferring the meaning of data by observing its flow.	P

B. Attacks against confidentiality

Confidentiality refers to the non-disclosure of certain information that poses a threat to the privacy of the patient. Privacy refers to the right of holding information about oneself from others. The confidentiality of the physician-patient relationship is often governed not only by medical ethics but by law [23]. Therefore, providing security against confidentiality attacks is one of the basic requirements of a successful health monitoring system. Security against such attacks is also necessary for data integrity since, typically, a combination of attacks against confidentiality leads to attacks against integrity. Attacks related to confidentiality are listed in Table II.

C. Attacks against integrity

Data integrity means maintaining the reliability and the accuracy of data. In particular, it is necessary to be able to detect any improper changes. Since false data can lead to dangerous situations [16], data integrity is critical for a medical application. Table III lists attacks related to data integrity.

D. Attacks against availability

Availability means that relevant data produced by the system is available when needed. In a medical application, compromise to data availability can cause medical alerts to be delayed or blocked. Attacks against availability typically

TABLE III. ATTACKS AGAINST INTEGRITY

Attack	Description	Active(A)/ Passive(P)
Modification	Modification of transmitted data.	A
Injection	Inserting false messages into the network.	A
Replay	Inserting valid but old messages into the network.	A
Selective unfairness	Blocking access to the medium from selected nodes. This can create a bias in the data.	A

TABLE IV. ATTACKS AGAINST AVAILABILITY

Attack	Description	OSI Layer
Jamming	Disrupting radio signals	Physical
Collision	Deliberate transmission of packets simultaneously to another node	Data link
Unfairness	A malicious node ignores the medium access protocol and hogs the medium to itself	Data link
Corrupted routing information	Alter the routing information to create for example routing loops.	Network
Wormhole	A malicious node advertises to have the shortest route after which all traffic is directed through the node [25].	Network
Black hole	Instead of relaying a packet to the next node in the route, the packet is dropped [26].	Network
Grey hole	Black hole attack in which packets are dropped selectively to complicate detection.	Network
Sybil	A malicious node poses as multiple nodes [27]. Can lead to several DoS attacks.	Network
De-synchronization	Interrupting a communication between nodes to cause them to be desynchronized and causing a sequence of retransmissions.	Transport
Sleep deprivation	A packet is sent to node at certain time intervals to prevent it from sleeping and thus draining its battery [28].	Transport
Barrage	A node is overwhelmed with legitimate requests to drain its battery [29].	Transport
Flooding	Deliberate congestion of the network with packets. There are many types of flood attacks such as the HELLO flood [26].	Several

disrupt the transmission of messages. These attacks can be realized in several Open Systems Interconnection (OSI) layers using different denial-of-service (DoS) attacks such as, for example, jamming and flooding. Table IV lists attacks against data availability with their relevant OSI layers. Each of these attacks is active. Corrupted routing information, wormhole, black hole, grey hole and Sybil attacks can be classified as routing attacks. Some of them apply only to a multi-hop network.

IV. THREAT ANALYSIS

In this section, the most relevant threats to each tier are identified. The general characteristics of Tiers 1 and 2 are similar. Both are wireless communication networks where data is channeled through a gateway. In general, the same threats apply to both of the tiers. However, the radio range and typical network topology of the tiers are different. Due to these reasons, threats that apply to Tier 1 also apply to Tier 2. Tier 3, on the other hand, is characterized by traditional computer and network security with well-established security mechanisms [30], [31].

Considering data integrity and confidentiality, hardware compromise needs to be addressed at every point of the chain. Data processing is often distributed, and may take place in various devices on Tiers 2 and 3. Analysis of ECG in a smartphone [32], fall detection from the accelerometer signal in a separate portable device [33], or decisions based on data fusion from several sources [34] are all examples of tasks that can be performed at different steps of the communication chain. This means that end-to-end encryption from a sensor to the end server cannot be applied until homomorphic encryption becomes feasible [35].

Additionally, various data standards [36]–[38] are utilized to meet the different requirements at the early and late communication chain. As a prominent example, the Continua Health Alliance has published a 3-tiered end-to-end set of standards for personal health device communication with a different data standard used at each interface [39]. Its recommendation includes the use of ISO/IEEE11073 (binary), HL7v2 (delimited text), and HL7 CDA (XML) at subsequent tiers; these changes require unpacking and remapping the included fields.

Relevant threats and the security requirements by the tier have been listed at Table V. See [40] for defenses related to sensor networks.

A. Tier 1

The intra-WBAN tier consists typically of nodes having limited battery and processing power. The network topology is fixed [21], [22]. Due to limited power, the WBAN radio range is also limited which restricts attacks based on the interception of radio signals. This effectively means that tracking threats require physical proximity to the patient and can be thus considered infeasible. However, assuming such systems are widely used, eavesdropping and traffic analysis of random people could be possible at public places. Therefore, such attacks need to be accounted for. Due to fixed network topology, routing threats do not apply to this tier.

The recent IEEE802.15.6 standard [22] designed for devices operating on this tier provides authentication, encryption and data freshness as its security mechanisms. These security mechanisms are adequate to counter most of the relevant attacks at this tier. The exceptions are compromise attacks as well as attacks against availability such as jamming and the collision attack. Availability attacks need to be countered with spread spectrum techniques [41].

B. Tier 2

Tier 2 encompasses a variety of different devices such as smartphones and laptops that have better processing power and battery capacity compared with devices on Tier 1. In addition, the radio range of this tier is greater rendering it more easily accessible for outsiders. For example, Bluetooth signals can be intercepted as far as over a kilometer away using specific antennas [42] (BlueSniper). Therefore, tracking threats become relevant in this tier. In addition, network topology is not fixed which creates possibilities for routing attacks. The gateway device could also be vulnerable to mobile malware, especially if a smartphone is used [43].

Tier 2 has the greatest number of security requirements. This is mainly due to the number of routing attacks that can be mounted on this tier. There are many ingenious secure routing solutions, such as [26], but not all security concerns are yet

TABLE V. RELEVANT THREATS BY TIER AND SECURITY REQUIREMENTS

Security threat	Tier	Security requirement / Defense
Selective unfairness	1	Robust data combination
Node impersonation	1,2	Entity authentication
Jamming	1,2	Spread spectrum
Collision	1,2	Spread spectrum, error correction
Unfairness	1,2	Frame limitation
Barrage	1,2	Secure clustering [29]
Sleep deprivation	1,2	Secure clustering
Hardware compromise	1,2,3	Tamper resistance
Software compromise	1,2,3	Secure coding
Subversion	1,2,3	System hardening, integrity checks
Eavesdropping	1,2,3	Encryption
Patient impersonation	1,2,3	Entity authentication
Side channel attacks	1,2,3	Side channel testing
Traffic analysis	1,2,3	Traffic randomness
Modification	1,2,3	Message authentication
Injection	1,2,3	Message authentication
Replay	1,2,3	Data freshness
Flooding	1,2,3	Client puzzles, cookies, ingress and egress filtering
Location tracking	2	Location privacy
Corrupted routing information	2	Secure routing
Wormhole	2	Secure routing
Black hole	2	Secure routing
Grey hole	2	Secure routing
Sybil	2	Secure routing
Desynchronization	2	Entity authentication
Malware	2,3	Malware protection
Man-in-the-middle	2,3	Entity authentication
Condition tracking	2,3	Traffic randomness
Social engineering	3	Security protocols and practices

accounted for. It is suggested that multi-hop is avoided in order to render some of the routing attacks inapplicable.

The IEEE802.15.4 standard [44] is designed to specify media access control for this tier. It provides basic security mechanisms such as confidentiality and protection against replay attacks. ZigBee defines a set of high level protocols on top of the IEEE802.15.4 standard. There are several issues with the security architectures of both IEEE802.15.4 and ZigBee [45]. For example, access control list is very limited.

Another possibility is to implement this tier using Bluetooth technology. However, many security problems have been identified for Bluetooth [46], [47]. There are also attacks that are specific to Bluetooth such as Bluejacking. Bluetooth does not provide security against man-in-the-middle or replay attacks. There are some security weaknesses shared by ZigBee and Bluetooth. Neither can, for example, provide location privacy since there are headers that are not encrypted. Security mechanisms provided by Bluetooth and Zigbee are not adequate to counter all of the relevant attacks of this tier. Another layer of security protocols is needed to provide location privacy and secure routing.

C. Tier 3

Tier 3 consists of communication over a public wired network. Routing attacks against multihop networks that are relevant to Tier 2 do not apply to Tier 3. However, denial-of-service attacks can be mounted in a distributive manner (DDoS) and it may be possible to exploit transitive trust [48]. Data is stored at the end server which means that access control mechanisms have to be implemented to keep it secure from eavesdropping and modification attempts. To limit access to the end server, a firewall configuration needs to be implemented. The end server also needs to be protected from hacking attempts by keeping its software up-to-date.

Tier 3 security is well established. There are many existing security mechanisms available for a wired network. It is possible to implement a virtual private network (VPN) that incorporates the gateway device, the end server as well as those machines that need to have access to the data. Security can be implemented on several OSI layers using, for instance, IPSec (network layer) and Transport Layer Security (TLS) / Secure Sockets Layer (SSL) (application layer).

Arguably the most serious threats at Tier 3 are caused by social engineering techniques. Such attempts may allow the attacker, for instance, to mount a subversion attack giving full access to the system and its data. In the worst case scenario, this is achieved in a covert way yielding such a breach hard to notice. To counter social engineering attacks, well maintained security protocols and practices are needed. Such practices need to be enforced for all personnel that have access to data.

V. CONCLUSION

Threats against the transmission chain of a medical health monitoring system were considered. Different attacks found in the scientific literature were classified based on threat to three basic security principles: confidentiality, integrity and availability. The transmission chain was considered as a 3-tiered structure and relevant threats were identified for each tier. It was noted that end-to-end security from a node to the end server is not possible due to distributed computing and incompatibility of existing data standards. Security requirements to counter the relevant attacks were also listed for each tier.

ACKNOWLEDGEMENTS

Research supported by Tekes, the Finnish Funding Agency for Technology and Innovation, as part of the ICMA project.

REFERENCES

[1] J. C. Matthews, D. Betley, F. Morady, and F. Pelosi, "Adverse interaction between a left ventricular assist device and an implantable cardioverter defibrillator," *J. Cardiovasc. Electrophysiol.*, vol. 18, no. 10, pp. 1107–1108, Sep 2007.

[2] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Security and Privacy, 2008 IEEE Symposium on*, 2008, pp. 129–142.

[3] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human scada system," Black Hat Conference presentation slides 2011, 2011.

[4] European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," http://eur-lex.europa.eu/ (retrieved 21.9.2012), 1995.

[5] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, Oct. 2004. [Online]. Available: http://dx.doi.org/10.1109/MPRV.2004.18

[6] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Department of Computer Science, University of Virginia, USA, Tech. Rep., 2006.

[7] T. Nijsen, P. J. M. Cluitmans, J. Arends, and P. Griep, "Detection of subtle nocturnal motor activity from 3-d accelerometry recordings in epilepsy patients," *Biomedical Engineering, IEEE Transactions on*, vol. 54, no. 11, pp. 2073–2081, 2007.

[8] A. Dalton, S. Patel, A. Chowdhury, M. Welsh, T. Pang, S. Schachter, G. OLaighin, and P. Bonato, "Development of a body sensor network to detect motor patterns of epileptic seizures," *Biomedical Engineering, IEEE Transactions on*, vol. 59, no. 11, pp. 3204–3211, 2012.

[9] K. Cuppens, L. Lagae, B. Ceulemans, S. Van Huffel, and B. Vanrumste, "Detection of nocturnal frontal lobe seizures in pediatric patients by means of accelerometers: A first study," in *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*, 2009, pp. 6608–6611.

[10] A. Salarian, H. Russmann, C. Wider, P. Burkhard, F. J. G. Vingerhoets, and K. Aminian, "Quantification of tremor and bradykinesia in parkinson's disease using a novel ambulatory monitoring system," *Biomedical Engineering, IEEE Transactions on*, vol. 54, no. 2, pp. 313–322, 2007.

[11] S. Patel, K. Lorincz, R. Hughes, N. Huggins, J. Growdon, D. Standaert, J. Dy, M. Welsh, and P. Bonato, "A body sensor network to monitor parkinsonian symptoms: extracting features on the nodes," in *5th International Workshop on Wearable Micro and Nanosystems for Personalised Health, pHealth2008*, 2008, pp. 21–23.

[12] L. Palmerini, L. Rocchi, S. Mellone, F. Valzania, and L. Chiari, "Feature selection for accelerometer-based posture analysis in Parkinson's disease," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 15, no. 3, pp. 481–490, 2011.

[13] N. L. Keijsers, M. W. Horstink, and S. C. Gielen, "Ambulatory motor assessment in parkinson's disease," *Movement Disorders*, vol. 21, no. 1, pp. 34–44, 2006. [Online]. Available: http://dx.doi.org/10.1002/mds.20633

[14] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4, pp. 307–326, 2006.

[15] A. Pantelopoulos and N. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 40, no. 1, pp. 1–12, 2010.

[16] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011. [Online]. Available: http://www.mdpi.com/1424-8220/12/1/55

[17] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *Systems and Networks Communications, 2006. ICSNC '06. International Conference on*, 2006, pp. 40–40.

[18] T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in *Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on*, oct. 2008, pp. 1–5.

[19] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Communications, IEEE*, vol. 17, no. 1, pp. 51–58, 2010.

[20] E. Shi and A. Perrig, "Designing secure sensor networks," *Wireless Communications, IEEE*, vol. 11, no. 6, pp. 38–43, 2004.

[21] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile Networks and Applications*, vol. 16, no. 2, pp. 171–193, Apr. 2011. [Online]. Available: http://dx.doi.org/10.1007/s11036-010-0260-8

[22] "IEEE standard for local and metropolitan area networks - part 15.6: Wireless body area networks," *IEEE Std 802.15.6-2012*, pp. 1–271, 2012.

[23] Office for Civil Rights, United State Department of Health and Human Services, "Medical privacy. national standards of protect the privacy of personal-health-information," http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html (retrieved 29 April 2013).

[24] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Security and Privacy, 2005 IEEE Symposium on*, may 2005, pp. 49 – 63.

[25] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 370–380, 2006.

[26] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293 – 315, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870503000088

[27] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. London, UK, UK: Springer-Verlag, 2002, pp. 251–260. [Online]. Available: http://dl.acm.org/citation.cfm?id=646334.687813

[28] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proceedings of the 7th International Workshop on Security Protocols*. London, UK, UK: Springer-Verlag, 2000, pp. 172–194. [Online]. Available: http://dl.acm.org/citation.cfm?id=647217.760118

[29] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. T. Kandemir, and R. R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006.

[30] N. Doraswamy and D. Harkins, *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 1999.

[31] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation," *Communications Magazine, IEEE*, vol. 42, no. 10, pp. 146–154, 2004.

[32] J. Oresko, Z. Jin, J. Cheng, S. Huang, Y. Sun, H. Duschl, and A. Cheng, "A wearable smartphone-based platform for real-time cardiovascular disease detection via electrocardiogram processing," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 14, no. 3, pp. 734–740, 2010.

[33] M. Estudillo-Valderrama, L. Roa, J. Reina-Tosina, and D. Naranjo-Hernandez, "Design and implementation of a distributed fall detection system – personal server," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 13, no. 6, pp. 874–881, 2009.

[34] C. Bellos, A. Papadopoulos, R. Rosso, and D. Fotiadis, "CHRONIOUS: A wearable platform for monitoring and management of patients with chronic disease," in *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, 2011, pp. 864–867.

[35] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain," *Signal Processing Magazine, IEEE*, vol. 30, no. 2, pp. 108–117, 2013.

[36] National Electrical Manufacturers Association, "Digital Imaging and Communications in Medicine (DICOM) Part 1: Introduction and Overview," http://medical.nema.org/standard.html (retrieved 12.10.2012), 2011.

[37] P. Schloeffel, T. Beale, G. Hayworth, S. Heard, and H. Leslie, "The relationship between CEN 13606, HL7, and openEHR," in *Health Informatics Conference*, 2006.

[38] "ISO/IEC/IEEE Health informatics–Personal health device communication–Part 20601: Application profile–Optimized exchange protocol," *ISO/IEEE 11073-20601:2010(E)*, pp. 1–208, 2010.

[39] Continua Health Alliance, "Continua Design Guidelines Version 2011," 2011.

[40] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Communications Surveys Tutorials, IEEE*, vol. 8, no. 2, pp. 2–23, 2006.

[41] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, no. 3, pp. 41–47, 2006.

[42] P. McFedries, "Bluetooth cavities," *IEEE Spectrum*, vol. 42, no. 6, p. 88, 2005.

[43] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *Security and Privacy, 2012 IEEE Symposium on*, 2012, pp. 95–109.

[44] "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, 2011.

[45] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *Proceedings of the 3rd ACM workshop on Wireless security*, ser. WiSe '04. New York, NY, USA: ACM, 2004, pp. 32–42. [Online]. Available: http://doi.acm.org/10.1145/1023646.1023654

[46] M. Jakobsson and S. Wetzel, "Security weaknesses in Bluetooth," in *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*, ser. CT-RSA 2001. London, UK, UK: Springer-Verlag, 2001, pp. 176–191. [Online]. Available: http://dl.acm.org/citation.cfm?id=646139.680779

[47] D. Singelée and B. Preneel, "Review of the Bluetooth security architecture," *Information Security Bulletin*, vol. 11, pp. 45–53, 2006.

[48] V. Ramasubramanian and E. G. Sirer, "Perils of transitive trust in the domain name system," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, ser. IMC '05. Berkeley, CA, USA: USENIX Association, 2005, pp. 35–35. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251086.1251121