12-3-2012

Forensic Readiness for Wireless Medical Systems

Brian Cusack
Edith Cowan University

Ar Kar Kyaw
AUT University

DOI: 10.4225/75/57b3af0efb860
10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

FORENSIC READINESS FOR WIRELESS MEDICAL SYSTEMS

Brian Cusack[1] and Ar Kar Kyaw
AUT University, Auckland, New Zealand
[1] SRI - Security Research Institute, Edith Cowan University, Perth, Western Australia
brian.cusack@aut.ac.nz; akk_mdy@yahoo.com

Abstract
Wireless medical devices and related information systems are vulnerable to use and abuse by unauthorized users. Medical systems are designed for a range of end users in different professional skill groups and also people who carry the devices in and on their bodies. Open, accurate and efficient communication is the priority for medical systems and as a consequence strong protection costs are traded against the utility benefits for open systems. Flexible security provisions are required and strong forensic capabilities built into the systems to treat the risk. In this paper we elaborate the problem area and discuss potential solutions to ready a medical system for the trade-off of open and secure services.

Keywords
Forensic Readiness, Security, Medical Systems, Wireless Networks

INTRODUCTION

The main focus of this research is the treatment of criminal risk with wireless medical devices and related systems in a medical healthcare environment. The deployment of wireless communications in the medical healthcare environment has rapidly increased for efficiencies and to meet enhanced clinical requirements (Nita et al., 2011; Paquette, 2011; Topol, 2011). Many medical devices such as telemetry, pulse oximetry monitors, electrocardiography (ECG) carts, neuro-stimulators, infusion pumps, insulin pumps, pacemakers, implantable cardioverter defibrillators (ICD) and drug pumps all have been moved to wireless communication technologies. The big advantage is the continuous monitoring of users' health in the real-time by automated equipment (Arney et al., 2011; Sagahyroon et al., 2011; Ren et al., 2010; Censi et al., 2010; Petkovic, 2009; Meingast et al., 2006).

However, the nature of wireless networking has inherited security and privacy problems. In addition the health care environment has requirements of open communication between professionals and between professionals and customers – who are often mobile between diverse geographic locations (for example a person who has a pacemaker inserted in their heart is free to travel globally but may require medical assistance in a remote location). Similarly within hospitals the 24 x 7 care requirement has a variety of arrangements between professional groups to maintain the continuity of service. Even with these challenges the deployment of wireless technologies in the medical healthcare industry has delivered benefits (Hanna et al., 2011; Devaraj & Ezra, 2011; Censi et al., 2010). The risk of such application is both of technical functionality and services misuse. The medical devices have generated security vulnerabilities leading to incidents for patients due to malfunction, misuse and the unauthorized hacking in wireless devices and communication protocols. For instance, Radcliffe (2011) has demonstrated hacking wirelessly into a commercially available insulin pump, which controls the insulin dosages for patients who have diabetics. Likewise, Halperin et al (2008, p. 1) have performed a number of "*software radio-based attacks*" on implantable cardioverter defibrillators (ICDs). Such types of attack can compromise patient safety, patient privacy and practitioner legal liability.

This paper is to give an introduction to the types and architectures of wireless technologies and systems that are used in medical environments. The systems are assessed for security problems that can have consequence for privacy breaches and material harm to system users. The discussion is limited to elaborating potential risks and potential risk treatments. The concern of making these open systems ready for investigation is approached from the perspective of adding to the systems and implementing resources that can store evidence on the system use.

MISUSE OF WIRELESS MEDICAL SYSTEMS

A misuse can be defined as a negative *"behaviour that is not allowed in the proposed system"* (Sindre & Opdahl, 2005; cited in Smith et al., 2010, p. 3). For instance, a misuse can be referred when a malicious hacker attacks on a wireless medical systems like an insulin pump system to compromise patient safety by stopping or changing the dosage of drug-administration. While all care is taken to protect a patient the Information Technology (IT) system has the potential to kill or harm a patient through misuse or deliberate abuse of the capability. The security risk of wireless medical devices and networks used in medical healthcare sector have

been established in the literature (Cagalaban & Kim, 2011; Gollakota et al., 2011; Arney et al., 2011; Hanna et al., 2011; Huang & Segal, 2011; Maisel & Kohno, 2010; Al Ameen et al., 2010; Denning et al., 2010; Saleem et al., 2010; Fu, 2009; Malasri & Wang, 2009; Denning et al., 2009; Zhang et al, 2003). There is a potential to alter dosages and to stop or interrupt the devices from normal operations and compromise the patient safety. However, the current literature stops at protection (IT security) and little is done regarding preserving evidence left after the wireless medical devices and IT system have been compromised. Hence, the forensic readiness in wireless medical devices is critical. Likewise, RFID enabled wireless medical systems applied for patients' monitoring or tracking in the hospitals can be exploited by a malicious hacker using one of potential attacks on implantable identification devices (IIDs) such as the cloning attack (Malasri & Wang, 2009). The IIDs are commonly implantable RFID tags with no power and vulnerable to threats. Hence, the attacker can compromise the privacy of the patients when patient unique IDs are obtained by using external RFID scanner. Table 1 lists such potential misuses of the technologies. The deployment of wireless technologies in the healthcare setting can not only offer benefits to the healthcare professionals but also to patients, while the pervasiveness of wireless medical devices and applications may possibly lead to potential misuse cases (Pyrek, 2011). Hasen and Hasen (2010) described the potential adverse events that could occur by using various implantable medical devices. For instance, the use of pacemaker or implanted cardiac defibrillator or ventricular assist device could lead to heart failure, arrhythmia, tachycardia and bradycardia. The nature of wireless networks allows potential threats and attacks to materialize that would have better treatment of risk in other types of communication network (Ngobeni et al., 2010).

Class	Description	Misuse Example
Wireless detection and connection	Misuse involves an intruder using the wireless medium as a tool to commit other criminal activities	Unauthorized use of WLAN or use of the WLAN as a launch pad for other criminal activities
Concealment of digital evidence	Misuse involves hidden wireless devices or hidden wireless networks	Fake access points
WLAN as an attack vector	Misuse involves attacks against the devices originated from the wireless network and then attacks against the WLAN medium itself	Rogue access point, Man-in-the-Middle attacks

Table 1 Classifications of WLAN misuse (adapted from Ngobeni et al., 2010, p. 108)

TYPES OF WIRELESS MEDICAL NETWORKS

Figure 1 shows the different types of wireless network based on span that are used in medical environments. Even though different types of technologies are being used in medical or healthcare industry, the following eight descriptions provide a comprehensive introduction: the Wireless Sensor Networks (WSN), Wireless Body Area Networks (WBANN), Wireless Personal Areal Networks (WPAN), Wireless Local Area Networks (WAN), Wireless Wide Area Networks (WWAN), General packet radio service (GPRS), Universal Mobile Telecommunications System (UMTS), and Radio Frequency Identification (RFID).

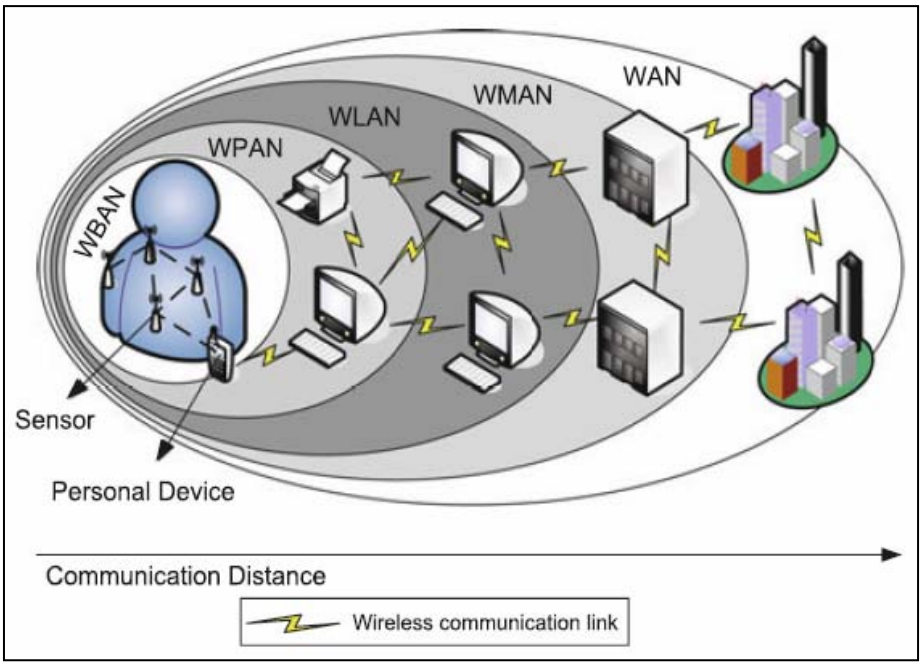

Figure 1 Medical wireless networks (Latre` et al., 2011, p. 6)

Wireless Sensor Networks (WSNs)

Wireless sensor networks (WSNs) are gaining popularity in the deployment of healthcare applications as a result of patients' tracking and real-time monitoring. It is performed by using low-cost, low-power sensor nodes deployed either inside the phenomenon or very close to it (Al Ameen et al., 2010; Yick et al., 2008; Sohraby et al., 2007; Ng et al., 2006; Akyildiz et al., 2002, p. 102). Darwish and Hassanien (2011) state that a WSN typically consists of a large number of sensor nodes which are equipped with on-board processors, communication and storage capabilities to collect and process significant information from the environment or phenomenon being monitored. For instance, a sensor node can use its processing ability to perform *"simple computations and transmit only the required and partially processed data"* (Darwish & Hassanien, 2011, p. 5566). However, sensor nodes in a WSN may have not only different sensing and storage capabilities (e.g., optical or magnetic), but also different communication technologies used (e.g., infrared or radio frequency) and data transfer rates (Dargie & Poellabauer, 2010). Similarly, Sohraby et al (2007, p. 1) says that *"a distributed or localised sensor, an interconnecting network, a central point of information clustering and a set of computing resources at the central point or beyond"* are four fundamental elements of a sensor network (SN). Furthermore, the commercial WSNs can also be classified into two categories such as *Category 1 WSNs (C1WSNs)* and *Category 2 WSNs (C2WSNs)* (Sohraby et al, 2007, p. 7).

Table 2 Categories of wireless sensor networks (adapted and simplified from Sohraby et al, 2007, pp. 7-11; Darwish & Hassanien, 2011, pp. 5567-5568)

	C1WSNs	***C2WSNs***	***Applications* [examples]**
Topology	Multi-point-to-point (Mesh-based)	Point-to-point, (star-based)	**Military** [monitoring forces, targeting, enemy tracking, biological attack detection, etc.,] **Environmental** [forest fire detection, flood detection, etc.,] **Health** [drug administration, monitoring of
Radio connectivity between wireless networks	Multi-hop	Single-hop	
Routing over the wireless network	Dynamic	Static	
Example	Military theatre systems	Residential control systems	

Supported Applications	Highly distributed high-node-count applications like environmental monitoring and national security systems	Confined short-range spaces such as a home, a factory, a building or human body	patients (remote or inside a hospital), etc.,] **Home / Residential** [home automation, automated meter reading, etc.,] **Commercial** [inventory control, vehicle tracking and detection, traffic flow surveillance, etc.,]
Type of data flow	High-data-rate	Low-data-rate	
Standard	ZigBee/IEEE 802.15.4	ZigBee/IEEE 802.15.4	
Frequency	2.4 GHz; Industrial, scientific and medical (ISM) radio band	2.4 GHz; Industrial, scientific and medical (ISM) radio band	
Data transmission rate	Up to 250 kbps	Up to 250 kbps	
Distance	30 – 200 ft	30 – 200 feet	

Wireless Body Area Networks (WBANs)

The emergent use of WBANs in the healthcare industry, especially in the fields of patient monitoring systems, is growing not only due to the advancement in wireless communication technologies, but also due to the development in wearable and implementable devices or sensors (Khan et al., 2012; Jain, 2011; Latre` et al., 2011; Liolios et al., 2010; Lim et al., 2010). WBANs are typically deployed within a range of 1 to 2 meters. By deploying WBANs, an extensive group of novel applications such as "*ubiquitous health monitoring (UHM), computer-assisted rehabilitation an emergency medical response system (EMRS)"* are enabled to improve the quality of life (Latre` et al., 2011; Li et al., 2010, p. 51). For instance, the real-time monitoring of patients who suffer from diseases such as diabetes, cardio vascular diseases (CVDs) and the like can be performed remotely and continuously whether or not the patients are in the hospital or at home (Khan et al., 2010; Latre` et al., 2011; Li et al., 2011; Li et al., 2010). In general, a WBAN is made up of a large number of intelligent devices that are tiny and normally implanted in or place on the body, and are capable of continuous monitoring of patient's physiological activities (Yuce & Khan, 2012; Chen et al., 2011; Latre` et al., 2011; Li et al., 2010).

Latre` et al (2011, p. 2) states that *sensors* and *actuators (or actors)* are two types of devices used in BANs in order *"to measure certain parameters of human body either externally or internally"* and *"to take some specific actions according to the data received from the sensors or through interaction with the user"*, respectively. For example, the measurement of the heart beat or temperature of the body can be done by a sensor device. Likewise, a handheld device such as personal digital assistant (PDA) or a laptop or a smart phone can be operated as a sink to perform interaction between the wireless sensor device and the patient or doctor (Latre` et al., 2010). A sink node can either be mobile or fixed and thought of as a gateway between a WBAN and external network (Muhammad et al., 2005). Hence, the patient related data collected from body-attached or implanted sensors can then be transferred from a sink to a centralised medical database (Li et al., 2010).

Wireless Personal Area Networks (WPANs)

According to Noorzaie (2006), short range networks like WPANs using IEEE 802.15.4 or Bluetooth can be potentially deployed in the medical or healthcare industry (Chevrollier & Golmie, 2005; Golmie et al., 2005). For instance, WPANs can be used by nurses or doctors at the hospitals in order to monitor patients in real-time instead of visiting patients' room frequently. Hence, nurses and doctors can have more opportunity to look after patients by saving time. In fact, WPANs can also be used to interconnect multiple devices within the hospital as the data collected from the patients can be transferred from one wireless device to another without performing data transferred manually by nurses or doctors (Noorzaie, 2006).

Wireless Local Area Networks (WLANs)

The Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802) designed the original WLAN 802.11 standard in 1997 for 1 Mbps to 2 Mbps wireless communication in the public frequency band of 5GHz and 2.4GHz (Hoglund, 2007; Karygiannis & Owens, 2002). As a result of flexibility, low cost, mobility and simplicity in operation, the deployments of WLANs have been rapidly

growing and widely utilised in enterprises, homes, universities, cafés, airports and hospitals over the last decade (Witters, 2011; Ngobeni et al., 2010; Heslop et al., 2010; Achi et al., 2009; Cypher et al., 2006; Banitsas et al, 2002). Unlike a traditional wired LAN, a WLAN or *wireless Ethernet* provides two or more end-user devices can communicate each other without requiring physical cabling by using Radio Frequency or Infra-Red technologies (Achi et al., 2009; Karygiannis & Owens, 2002). A WLAN mainly consists of two types of wireless devices such as a wireless station (e.g., laptop or PDA) and a wireless access point (WAP), and it is usually implemented as an extension to wired LAN (Scarfone et al. 2008, Varshney, 2003; Karygiannis & Owens, 2002). However, the typical indoors-connectivity range of IEEE 802.11 devices is up to 50 to 100 meters even though the greater connectivity range can be achieved in outdoors (Scarfone et al., 2008). Similarly, Chen et al (2004, p.1) state that WLANs are considered to be *"the next generation of clinical data network"* due to the prospect of capturing patients' clinical data that can be sent to a doctor or centralised patient database of the hospital by using different wireless devices like laptops, tablet computers, smart phones, PDAs or pagers (Newbold, 2004). For instance, 802.11 WLANs are being deployed to perform continuous monitoring of patients at home or in a hospital (Vassis et al., 2010; Lin et al., 2004; Varshney, 2003). In other word, the *"pervasive health monitoring, intelligent emergency management system, pervasive healthcare data access and ubiquitous mobile telemedicine"* can be carried out by deploying WLANs to fulfill the vision of *"Pervasive Healthcare"* (Malasri et al., 2009; Varshney, 2007, p. 113).

Wireless Wide Area Networks (WWANs) / GPRS / UMTS

Nowadays, the deployment of pervasive wireless technologies such as WWANs, GPRS and UMTS can be possible to monitor or transfer vital data of patients in the field of medical or healthcare industry. For instance, *MobiHealth* project was initiated in Europe in order to establish *"a generic platform for home healthcare using BAN-based sensors and GPRS or UMTS"* (for WWANs connectivity) wireless communication technology (Noorzaie, 2006, p. 8). Consequently, healthcare professionals have the benefits of monitoring outpatients remotely. On the other hand, outpatients who wear wireless body sensor devices can also take advantage of improve mobility and reduce the disruption to daily life.

Radio Frequency Identification (RFID)

RFID (radio frequency identification) technology can provide not only to identify the objects or people, but also provide healthcare professionals to have precise aces to the patient physiological data by using wireless radio communication (Liu et al., 2011; Yao et al., 2011; Hunt et al., 2007). As every system has its own essential components in order to operate successfully, a typical RFID system consists of three main components such as an RFID tag (active or passive) device, which is sometimes referred to as a transponder, RFID reader (or transceiver) and a host or controller which is connecting to an enterprise system (Roberts, 2006; Xiao et al., 2007; Hunt et al., 2007). RFID tag devices can be used to also track the patients and medical equipment in a hospital (Parlak et al., 2012; Noorzaie, 2006). The successful deployment of RFID systems in hospitals or healthcare industry (see Figure 2.3) was stated in the *"Evaluation the business value of RFID: Evidence from five case studies"* (Tzeng et al., 2008, p. 601). For instance, a RFID system was used for an emergency room by tagging patients with passive tags that stored patients' identification numbers (IDs) to track patients and monitor patients' physiological signals. Likewise, *"RFID smart medical platform"* was used in one of the hospital in Taiwan to identify new born babies with active RFID tags (Tzeng et al., 2008, p. 607). Hence, the nurses or doctors can access medical information related to patients by using wireless devices like PDAs or smartphones after the RFID reader has validated patients' IDs.

Hospital ID	Year of assess-ment	Primary technology in RTLS	Purpose of RTLS
01	2007	RFID	Patient ID in surgery
02	2007	A. RFID	A. Asset tracking
		B. Ultrasound	B. Patient tracking
03	2007	RFID	Asset tracking
04	2007	RFID	A. Asset tracking
			B. Personnel tracking
06	2007	RFID	Patient ID in ED
07	2007	ZigBee	Asset tracking
08	2007	RFID	Patient ID for delivering medicine
09	2007	RFID	Patient tracking
10	2007	RFID	Asset tracking
15	2007	Ultrasound	Asset tracking
16	2007	Ultrasound	A. Patient tracking
			B. Personnel tracking
11	2008	IR	A. Asset tracking
			B. Patient tracking
			C. Personnel tracking
05	2009	RFID	A. Asset tracking
			B. Temperature monitoring
12	2009	RFID	Asset tracking
13	2009	RFID	Patient ID in surgery
14	2009	UWB	A. Asset tracking
			B. Patient tracking
			C. Personnel tracking
17	2009	RFID	Personnel tracking
18	2009	RFID	Asset tracking
19	2009	RFID	A. Asset tracking
			B. Patient tracking
20	2009	RFID	A. Asset tracking
			B. Temperature monitoring
21	2009	RFID	Asset tracking
22	2009	ZigBee	Asset tracking
23	2009	RFID	Asset tracking

Table 3 Wireless technologies used for RTLS in hospitals (simplified from Fisher & Monahan, 2012, p. 708)

DISCUSSION

Figure 2 shows a summative architecture for the monitoring of a human body in a hospital setting. The wireless connection of a human's most personal information is made into the medical information system that may extend beyond the immediate geographic location and access data storage facilities anywhere in a cloud network deployment. Similarly the hospital information system provides a push capability where the human vital statistics are controlled by feedback loops through the IT sensory systems. In both instances of push and pull, information risks to privacy and risks to life are exposed by the nature of the technology itself. In an ideal situation the technology delivers without fault, the users perform without error and no malicious activities occur. However in a forensically ready system the system and its potential effects have to be deconstructed and mapped against the risk criteria the industry has adopted. Immediately the risk of wireless communication systems security failure has to be factored into the preparation of a risk management plan. In Figure 3 the elements of disclosure and control risk are materialized by placing a hacker into the information systems architecture in a position where influence can be exerted onto privacy security and control security. As has been discussed above the requirement to have open communications with many system user groups works against strong security and hence breaches can be expected.

Figure 3 shows the architecture for system forensic readiness. A forensically ready system has security for prevention of events and forensic capability to investigate post events. The system architecture is enhanced by adding a forensic server to the hospital information system and also the deployment of drones within the wireless network. Drones are not visible to the wireless network users but they can track, trap and forward packets to the forensic server. RFID tagged elements within the medical system are also at risk of compromise from a range of attacks. Such events can be monitored by readers (fixed & mobile) and audited by mapping onto expected behaviours in the forensic server. In such a proposal the cost of information storage is balanced against the benefit of having the evidence and its ready availability. The utility cost to the service system is minimal as the forensic element is independent and self resourcing, and can function without visibility.

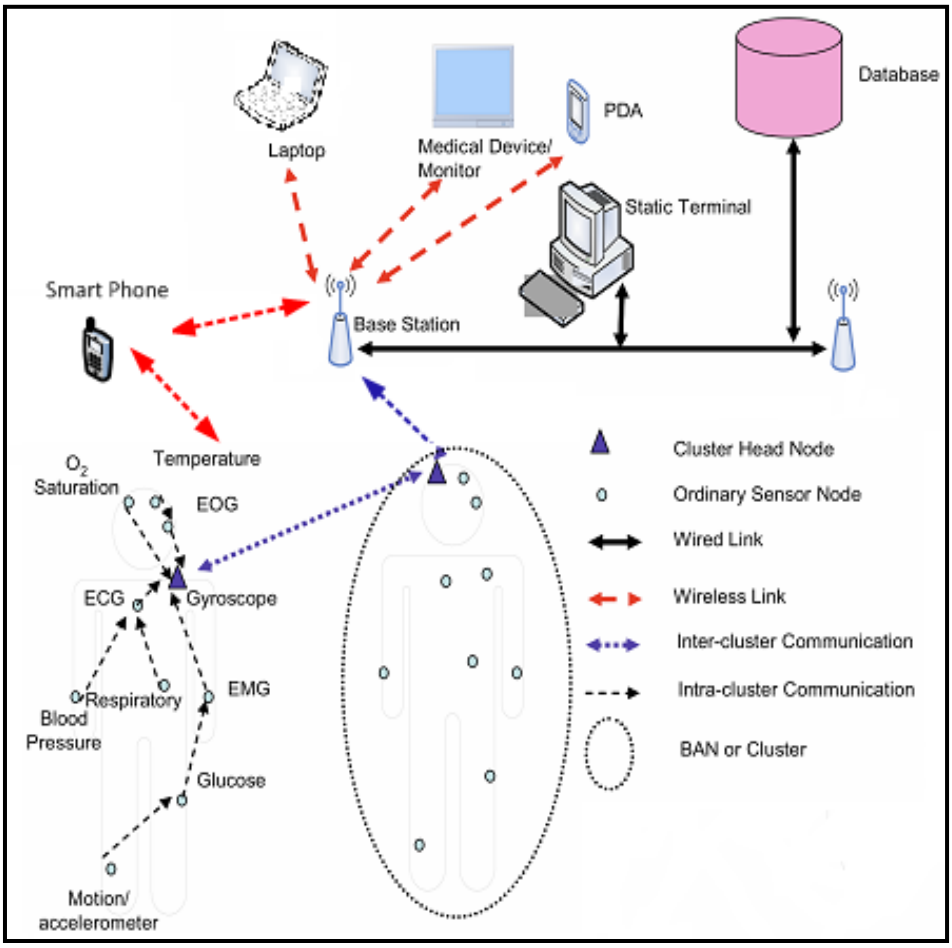

Figure 2 Continuous monitoring of patient's physiological activities by using BAN and WLAN (adapted from Chen et al., 2010, p.1)

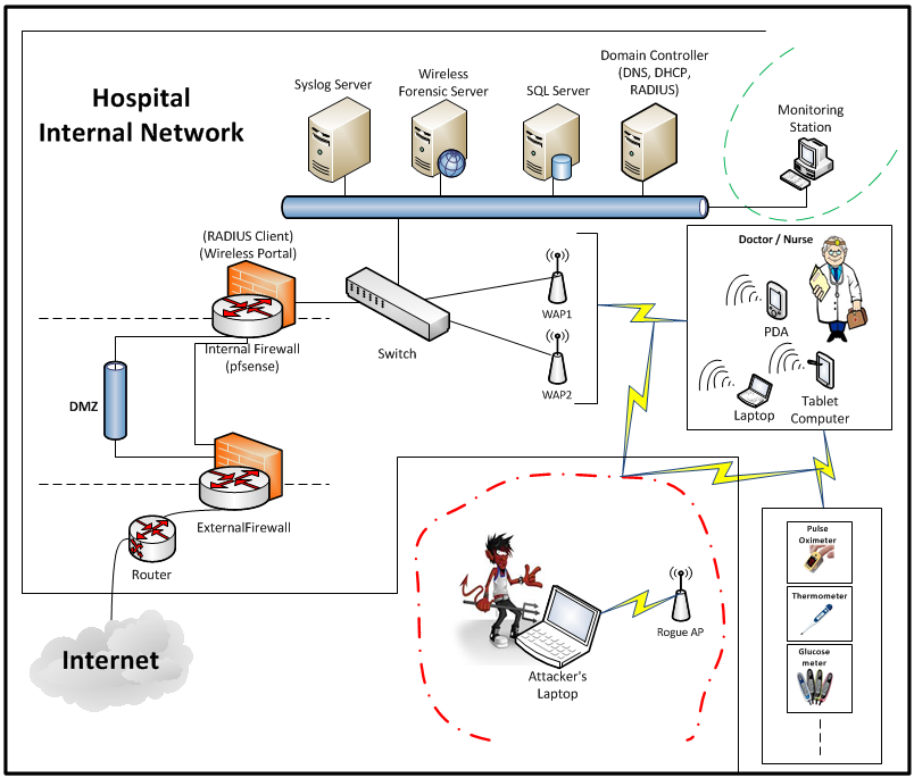

Figure 3 Proposed forensically ready hospital wireless network architecture

CONCLUSION

The adoption of wireless technologies in medical environments for medical device interaction and related information systems communications has increased the scope of possible problems that may arise from security breaches. The medical environment has requirements that cannot be satisfied by security provisions alone. Other researchers have shown that wireless security systems can be hacked and that the consequences for humans are fatal. The necessity of forensic readiness is a prudent risk treatment for such information systems. In this paper the medical uses of wireless communications has been reviewed in detail and a proposal for a forensically ready system made.

REFERENCES

Achi, H., Hellany, A., & Nagrial, M. (2009). Methodology and challenges in digital security forensics of wireless systems and devices. In G. Aly, H. Mahdi, A. Salem, M. W. El-Kharashi, A. B. El-Din, M. A. Sobh, & M. Taher (Eds.), *Proceedings of the International Conference on Computer Engineering & Systems, 2009, ICCES 2009* (pp. 283-287). Cairo, Egypt: IEEE. doi: 10.1109/ICCES.2009.5383266

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine, 40*(8), 102-114.

Al Ameen, M. Liu, J., & Kwak, K. (2010). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems, February*(2010), 1-9. doi: 10.1007/s10916-010-9449-4

Arney, D., Venkatasubramanian, K., Sokolsky, O. and Lee, I. (2011). Biomedical Devices and Systems Security. *Proceedings of 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC '11)*, Boston, MA, August/September, 2011.

Aubert, H. (2011). RFID technology for human implant devices. *Comptes Rendus Physique, 12*(7), 675-683. doi:10.1016/j.crhy.2011.06.004

Banitsas, K., Istepanian, R. S. H, & Sapal, T. (2002). Applications of medical Wireless LAN systems (MedLAN). *International Journal of Medical Marketing, 2*(2), 136-142.

Cagalaban, G., & Kim, S. (2011). *Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption*. Paper presented at the 2011 13th International Conference on Advanced Communication Technology (ICACT), Gangwon-Do, Korea (South).

Censi, F., Calcagnini, G., Mattei, E., Triventi, M., & Bartolini, P. (2010). *RFID in healthcare environment: Electromagnetic compatibility regulatory issues*. Paper presented at the 32nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS), 2010, Buenos Aires, Argentina.

Chen, B., Varkey, J. P., Pompili, D., Li, J. K. J., & Marsic, I. (2010). Patient Vital Signs Monitoring using Wireless Body Area Networks. In *Proceedings of the 2010 IEEE 36th Annual Northeast Bioengineering Conference* (pp. 1-2). New York, USA: Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/NEBC.2010.5458139

Chen, D., Soong, S., Grimes, G. J., & Orthner, H. F. (2004). Wireless local area network in a prehospital environment. *BMC Medical Informatics and Decision Making, 4*(12), 1-9. doi:10.1186/1472-6947-4-12

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. (2011). Body area networks: A survey. *Journal of Mobile Networks and Applications, 16*(2), 171-193. Germany: Springer. doi: 10.1007/s11036-010-0260-8

Cypher, D., Chevrollier, N., Montavont, N., & Golmie, N. (2006). Prevailing over wires in healthcare environment: benefits and challenges. *IEEE Communications Magazine, 44*(4), 56-63. doi:10.1109/MCOM.2006.1632650

Dargie, W., & Poellabauer, C. (2010). *Fundamentals of wireless sensor networks: theory and practice*. Singapore: John Wiley & Sons Ltd.

Darwish, A., & Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors,* 11(6), 5561-5595; doi:10.3390/s110605561

Denning, T. B. S., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Journal of Neurosurg Focus, 27*(1), E7.

Denning, T., B. S, A., Friedman, B., Gill, G. T., Kohno, T., & Maisel, W. H. (2010). Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices. *CHI '10 Proceedings of the 28th International Conference on Human Factors in Computing Systems,* 917-926. doi:10.1145/1753326.1753462

Devaraj, S. J., & Ezra, K. (2011). Current trends and future challenges in wireless telemedicine system. In S. A. Perumal (Ed.), Proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT), 6(2011), pp. 417-421. Hong Kong, China: Institute of Electrical and Electronics Engineers Inc.

Eren, T. (2006). *Wireless sensors and instruments: Network, design and applications*. Boca Raton, FL: Taylor & Francis Group, LLC.

Fisher, J. A., & Monahan, T. (2012). Evaluation of real-time location systems in their hospital contexts. *International Journal of Medical Informatics, 81*(10), 705-712. doi:10.1016/j.ijmedinf.2012.07.001

Freudenthal, E., Herrera, D., Kautz, F., Natividad, C., Ogrey, A., Sipla, J., ... Estevez, L. (2007). *Evaluation of HF RFID for implanted medical applications* [UTEP-CS-07-36]. Texax, El Paso: University of Texas, Department of Computer Science.

Fu, K. (2009). Inside risks: Reducing risks of implantable medical devices. *Communications of the ACM, 52*(6), 25-27. doi:10.1145/1516046.1516055

Garrett, B. M., & Jackson, C. (2006). A mobile clinical e-portfolio for nursing and medical students, using wireless personal digital assistants (PDAs). *Nurse Education Today, 26*(8), 647-654. doi:10.1016/j.nedt.2006.07.020.S0260-6917(06)00120-1

Golmie, N., Chevrollier, N., & Rebala, O. (2003, December). Bluetooth and WLAN coexistence_challengesand solutions. *IEEE Wireless Communications, 10*(6), 22-29. doi: 10.1109/MWC.2003.1265849

Grimes, S. L. (2011). Using 80001 to manage medical devices on the IT network. *Journal of Biomedical Instrumentation & Technology: Managing Medical Devices on the IT Network, 45*(s2), 23-26. doi: http://dx.doi.org/10.2345/0899-8205-45.s2.23

Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K. (2001, August). *They can hear your heartbeats: Non-invasive security for implantable medical devices*. Paper presented at the Conference of ACM SIGCOMM (SIGCOMM'11) 2011, Toronto, Ontario, Canada.

Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T., & Maisel, W.H. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In B. Werner (Ed.), *Proceedings of the 2008 IEEE Symposium on Security and Privacy, (pp. 129-142)*. Piscataway, New Jersey: the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers Inc.

Hanna, S., Rolles, R., Molina-Markham, A., Poosankam, P., Fu, K., & Song, D. (2011, August). *Take two software updates and see me in the morning: the case for software security evaluations of medical devices*. Paper presented at the 2nd USENIX Workshop on Health Security and Privacy, San Francisco, CA.

Hansen, J. A., & Hansen, N. M. (2010). A taxonomy of vulnerabilities in implantable medical devices. In *Proceedings of the second annual workshop on security and privacy in medical and home-care systems, SPIMACS '10* (pp. 13-20). New York, USA: ACM Press. doi: 10.1145/1866914.1866917

Heslop, L., Weeding, S., Dawson, L., Fisher, J., & Howard, A. (2010). Implementation issues for mobile-wireless infrastructure and mobile health care computing devices for a hospital ward setting. *Journal of Medical Systems, 34*(4), 509-518. doi: 10.1007/s10916-009-9246-y

Hoglund, D. (2007). Wireless technology infrastructure: A business strategy. *Journal of Biomedical Instrumentation & Technology, 41*(6), 457-460.

Huang, A. R., & Segal, B. (2011). *A literature review of the safety of medical body area network devices in magnetic resonance imaging*. Paper presented at the 5th International Symposium on Medical Information & Communication Technology (ISMICT), 2011, Montreux, Switzerland.

Jain, P. C. (2011). Wireless body area network for medical healthcare. IETE Technical Review, 28(4), 362-371. doi:10.4103/0256-4602.83556

Karygiannis, T. & Owens, L. (2002). *NIST Special Publication 800-48: Wireless Network Security – 802.11, Bluetooth and Handheld Devices*. Gaithersburg, Maryland: National Institute of Standards and Technology.

Khan, J. Y., Yuce, M. R., Bulger, G., & Harding, B. (2012). Wireless body area network (WBAN) design techniques and performance evaluation. Journal of Medical Systems, 36(3), 1441-1457. United States of America: Springer. doi:10.1007/s10916-010-9605-x

Kierkegaard, P. (2011). Electronic health record: Wiring Europe's healthcare. *Computer Law & Security Review, 27*(5), 503-515. doi:10.1016/j.clsr.2011.07.013

Latre`, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Journal of Wireless Networks, 17*(1), 1-18. doi:10.1007/s11276-010-0252-4

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications, 17*(1), 51-58.

Li, S., Hu, F., & Li, G. (2011). Advances and challenges in body area network. *Communications in Computer and Information Science, 226*(2011), 58-65. doi: 10.1007/978-3-642-23235-0_8

Lim, S., Oh, T. W., Choi, Y. B., & Lakshman, T. (2010). Security issues on wireless body area network for remote healthcare monitoring. In *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, (SUTC '10)*, pp. 327-332. doi: 10.1109/SUTC.2010.61

Lin, C.-C., Lee, R.-G., & Hsiao, C.-C. (2008). A pervasive health monitoring service system based on ubiquitous network technology. *International Journal of Medical Informatics, 77*(7), 461-469. doi:10.1016/j.ijmedinf.2007.08.012

Liolios, C., Doukas, C., Fourlas, G., & Maglogiannis, I. (2010). An overview of body sensor networks in enabling pervasive healthcare and assistive environments. In *Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environment* (pp. 43:1-43:10). New York, USA: ACM Press.

Liu, C. C. H., Chang, C.-H., Su, M.-C., Chu, H.-T., Hung, S.-H, Wong, J.-M, & Wang, P.-C. (2011). RFID-initiated workflow control to facilitate patient safety and utilization efficiency in operation theatre. *International Journal of Computer Methods and Programs in Biomedicine, 104*(3), 435-442. doi:10.1016/j.cmpb.2010.08.017

Maisel, W. H., & Kohno, T. (2010). Improving the security and privacy of implantable medical devices. *New England Journal of Medicine, 362*(13), 1164-1166. doi:10.1056/NEJMp1000745

Majchrowski, B. (2010, June). Real-time locating systems: Measuring the benefits. *Journal of Material Management in Health Care, 2010*(June), 18-20.

Malasri, K., & Wang, L. (2009). Securing Wireless Implantable Devices for Healthcare: Ideas and Challenges. *IEEE Communications Magazine, July*(2009), 74-80. Doi:10.1109/MCOM.2009.5183475

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with healthcare information technology. *In Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS '06* (pp. 5453-5458). New Yourk, USA: Institute of Electrical and Electronics Engineers Inc. doi:10.1109/IEMBS.2006.260060

Muhammad, S., Furqan, Z., & Guha, R. (2005). Wireless sensor network security: A secure sink node architecture. In *Proceedings of 24th IEEE International Performance, Computing, and Communications Conference, IPCCC, 2005* (pp. 371-376). Arizona, USA: ACM Press. doi:10.1109/PCCC.2005.1460590

Newbold, S.K., (2004, April). New uses for wireless technology. *The Nurse Practitioner, 29*(4), 46-46.

Ng, H. S., Sim, M. L., & Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal, 24(2),* 138-144. Retrieved from http://www.springerlink.com/content/61h5565851213349

Ngobeni, S., Venter, H., & Burke, I. (2010). A forensic readiness model for wireless networks. In K.-P. Chow, & S. Shenoi (Eds.), *Advances in Digital Forensics VI, IFIP AICT 377*(pp. 107-118). Germany: Springer.

Nita, L., Cretu, M., & Hariton, A. (2011). *System for remote patient monitoring and data collection with applicability on E-health applications*. Paper presented at the 2011 7th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania.

Noorzaie, I. (2006). *Survey paper: Medical applications of wireless networks*. Retrieved from http://www.cs.wustl.edu/~jain/cse574-06/medical_wireless.htm

Paquette, A. (2011). *Design of a pragmatic test lab for evaluating and testing wireless medical devices.* Paper presented at the Bioengineering Conference (NEBEC), 2011 IEEE 37th Annual Northeast, Troy, New York. Retrieved from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5778521

Paquette, A., Painter, F., & Jackson J. L. (2011, May-June). Management and risk assessment of wireless medical devices in the hospital. *Journal of Biomedical Instrumentation & Technology, 45*(3), 243-248.

Parlak, S., Sarcevic, A., Marsic, I., & Burd, R. S. (2012). Introducing RFID technology in dynamic and time-critical medical settings: requirements and challenges. *Journal of Biomedical Informatics, 45*(5), 958-974. doi:10.1016/j.jbi.2012.04.003

Petkovic, M. (2009). *Remote patient monitoring: Information reliability challenges*. Paper presented at the 9th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services, TELSIKS'09, Nis, Serbia.

Pyrek, K. M. (2011). *Healthcare crime: investigation abuse, fraud, and homicide by caregivers*. Boca Raton, FL: CRC Press.

Radadcliffe, J. (2011). Hacking Medical Devices for Fun And Insulin: Breaking The Human Scada System. *Paper Presented at The Black Hat Security Conference (USA 2011), Las Vegas, United States of America.*

Ren, Y., Pazzi, R. W. N., & Boukerche, A. (2010). Monitoring patients via a secure and mobile health system. *Journal of IEEE Wireless Communications, February*(2010), 59-65.

Saganyroon, A., Aloul, F., Al-Ali, A. R., Bahrololoum, M. S., Makhsoos, F., & Hussein, N. (2011). *Monitoring patients' signs wirelessly*. Paper presented at the Proceedings of 2011 1st Middle East Conference on Biomedical Engineering (MECBME), Sharjah, United Arab Emirates, 21-24 February 2011; pp. 283-286.

Saleem, S., Ullah, S., & Kwak, K. S. (2010). Towards security issues and solutions in Wireless Body Area Networks. In C. Yuan, L. Tsay, F. Wang, F. Ko, J. Zhan, Y. Na, Y. Sohn (Eds.), *Proceedings of the 6th International Conference on Networked Computing, INC2010* (pp. 1-4). Gyeongju, Korea (South): Institute of Electrical and Electronics Engineers, Inc.

Scarfone, K., Dicoi, D., Sexton, M., & Tibbs, C. (2008, July). *NIST Special Publication 800-48 Revision 1: Guide to Securing Legacy IEEE 802.11 Wireless Networks*. Gaithersburg, Maryland: National Institute of Standards and Technology.

Slay, J., & Turnbull, B. (2006). *The need for a technical approach to Digital Forensic evidence collection for wireless technologies.* Paper presented at the IEEE Information Assurance Workshop, West Point United States Military Academy, NY, 23 June 2006.

Smith, B., Austin, A., Brown, M., King, J., Lankford, J., Meneely, A., & Williams, L. (2010). Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. In *Proceedings of the second annual workshop on security and privacy in medical and home-care systems, SPIMACS '10* (pp. 1-12). New York, USA: ACM Press. doi: 10.1145/1866914.1866916

The National Science Foundation. (2012). *Wireless sensors: from medicine to motion*. Retrieved from http://www.nsf.gov/news/special_reports/liberty/03_technology_02.jsp

Topol, E. J. (2011). The digital wireless revolution: wireless devices and their applications in healthcare. *In Futurescan 2011: Healthcare trends and implication 2010-2015* (pp. 37-42). United States of America: Health Administration Press.

Turab, N., Aljawarneh, S., & Masadeh, S. (2010). A study of secure deployment of wireless technology in the medical fields. In *Proceedings of the 1st International Conference on Intelligent Semantic Web-Services and Applications* (ISWSA '10). New York, US: ACM. Article 25, 4 pages. doi:10.1145/1874590.1874615

Tzeng, S., Chen, W., Pai, F. (2008). Evaluating the business value of RFID: evidence from five case studies. *International Journal of Production Economics, 112*(2), 601-613. doi:10.1016/j.ijpe.2007.05.009

Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. *Journal of Medical Systems, 36*(3), 1065-1094. doi: 10.1007/s10916-010-9571-3

Varshney, U. (2003). Pervasive healthcare. *IEEE Computers, 36*(12), 138-140. doi:10.1109/MC.2003.1250897

Varshney, U. (2007). Pervasive healthcare and wireless health monitoring. *Journal of Mobile Networks and Applications, 12*(2-3), 113-127. doi:10.1007/s11036-007-0017-1

Vassis, D., Belsis, P., Skourlas, C., & Pantziou, G. (2010). Providing advanced remote medical treatment services through pervasive environments. *Journal of Personal and Ubiquitous Computing, 14*(6), 563-573. doi: 10.1007/s00779-009-0273-0

Witters, D. (2011). Wireless medical systems: Risks, challenges, and opportunities. *Journal of Biomedical Instrumentation & Technology: Managing Medical Devices on the IT Network, 45*(s), 49-52. doi: http://dx.doi.org/10.2345/0899-8205-45.s2.49

Yao, L., Liu, B., Wu, G., Yao, K., & Wang, J. (2011). A biometric key establishment protocol for body area networks. *International Journal of Distributed Sensor Networks, 2011*(2011), 1-10. doi:10.1155/2011/282986

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks, 52*(2008), 2292-2330. doi:10.1016/j.comnet.2008.04.002

Yuce, M. R., & Khan, J. Y. (2012). *Wireless body area networks: Technology, Implementation, and Applications*. Danvers, USA: Pan Stanford Publishing Pte. Ltd.

Zhang, J., Johnson, T. R., Patel, V. L., Paige, D. L., & Kubose, T. (2003). Using usability heuristics to evaluate patient safety of medical devices. *Journal of Biomedical Informatics, 36*(2003), 23-30. doi:10.1016/S1532-0464(03)00060-1