12-3-2014

Managing wireless security risks in medical services

Brian Cusack
Auckland University of Technology, brian.cusack@aut.ac.nz

Akar Kyaw
Auckland University of Technology, akar.kyaw@aut.ac.nz

Recommended Citation

Cusack, B., & Kyaw, A. (2014). Managing wireless security risks in medical services. DOI: https://doi.org/10.4225/75/5798208831b44

DOI: 10.4225/75/5798208831b44
3rd Australian eHealth Informatics and Security Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/aeis/18

MANAGING WIRELESS SECURITY RISKS IN MEDICAL SERVICES

Brian Cusack[1], Akar Kyaw[2]
[1,2]Auckland University of Technology
[1]brian.cusack@aut.ac.nz, [2]akar.kyaw@aut.ac.nz

Abstract

Medical systems are designed for a range of end users from different professional skill groups and people who carry the devices in and on their bodies. Open, accurate, and efficient communication is the priority for medical systems and consequently strong protection costs are traded against the utility benefits for open systems. In this paper we assess the vulnerabilities created by the professional and end user expectations, and theorise ways to mitigate wireless security vulnerabilities. The benefits of wireless medical services are great in terms of efficiencies, mobility, and information management. These benefits may be realised by treating the vulnerabilities and reducing the cost of adverse events. The purpose of this paper is to raise and to discuss key issues so that others may be motivated to treat the problems and to better optimise the trade-off for design improvement.

Keywords
Wireless, Security, Medical, Devices, Services, Safety.

INTRODUCTION

The deployment of wireless communications in medical healthcare environment has expanded to meet the clinical requirements (Nita, Creta & Hariton, 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, use the wireless communication technologies as these wireless medical devices allow the continuous monitoring of users' health in the real-time (Ren, Pazzi & Boukerche., 2010; Censi, Calcagnini, Matter, Triventi & Beutolini, 2010; Petkovic, 2009; Meingast, Ravsta & Sastry, 2006). Wireless services also allow mobility of patients, time-space flexibility for staff and automated information management. The staff-patient relationship is made less structured and more socially integrated so that health services are seen as a natural part of daily life (Arney, Venkata, Sokotsky & Lee, 2011; Sagahyroon, Aloul, Al-Ali, Bahrololoum, Makhsoos, & Hussein, 2011).

Wireless technologies enable the electronic devices to interconnect and communicate without having the need of physical wired cabling by using radio frequency transmissions (Karygiannis & Owens, 2002). As a result of advancement in wireless technologies, the prevalent adoptions of wireless networks offer numerous benefits to users and organizations (Turab, Aljawarneh, & Masadeh, 2010). These deployments of wireless sensor networks (WSNs), wireless personal area networks (WPANs), wireless local area networks (WLANs), and wireless body area networks (WBANs) have offered a significant enrichment in quality of life. In the industries of healthcare, retail, education and entertainment there has been improvement in mobility, flexibility and productivity (Yuce & Khan, 2012; Darwish & Hassanien, 2011; Turab et al., 2010). However, the nature of wireless networks also exposes the risks that may harm the users and reduce the potential benefits (Ngobeni, Venter & Burke, 2010; Radcliffe, 2011). The nature of wireless networking has inherited security and privacy problems (Halperin, 2008). In addition, the healthcare environment has requirements of open communication between professionals and patients who are often mobile between diverse geographic locations. Systems are not unified or standardised. Some common standards may be adopted but the variability in capability, proprietary hardware, and software, and policies make seamless services difficult. Even with these challenges, the deployment of wireless technologies in the medical healthcare has delivered benefits (Hanna, Rolles, Molina, Poosankam, Fu & Song, 2011; Devaraj & Ezra, 2011; Censi, Calcagnini, Mattei, Triventi & Bartolini, 2010). Our concern in this paper is the securing of these services in such a way that the potential for harm is minimised while the opportunity for patient benefits are maximised.

BACKGROUND LITERATURE

Security is an essential component of any IT system, either wired or wireless. The main difference between wired and wireless networks is the vulnerability at the physical layer (Cypher, Chevrollier, Montavont & Golmie, 2010). The wireless data transmitted in the wireless network is easily captured or eavesdropped by passive or active attackers. Consequently, built-in wireless security architectures, such as the IEEE 802.11 WLAN standards, and encryption protocols such as the WEP, WPA, RSN and WPA2 are required to protect and maximise the benefits from wireless networks (Karygiannis & Owens, 2002; Scarfone, 2008; Bulbul 2008). The security goals for wireless networks are the fundamental four of confidentiality, integrity, availability and authentication of users (Al & Yoshigoe, 2011). The vulnerabilities of wireless networks present risks for the use in any environment. Table 1 summaries the types of risks as threats a wireless network has on account of its hardware, software and configurations (adapted from Diksha & Shubham, 2006, pp. 2-3; Frankel, Eydt, Owens & Scarfone, 2007, p. 28). The identification of the risks allows management planning to assure the system benefits are greater than the costs, and in a medical system, all risk of potential impact on services is mitigated. In this way, adverse impacts on humans are treated and patient safety assured.

Table 1. Types of major threats against wireless networks and devices (adapted from Diksha & Shubham, 2006, pp. 2-3; Frankel et al., 2007, p. 28)

Threat Type	Description
Ad hoc or Peer-to-Peer Connection	Attacker can exploit a wireless client or device after establishing ad hoc connection (unauthorised client attempt to form ad hoc network with legitimate client). After establishing the ad hoc connection, the attacker can perform port scanning to explore and exploit client vulnerabilities
Client Mis-association	Attacker can compromise a corporate wireless client after the client within business premises mis-associates or connects to an unauthorised external Wi-Fi network (which is set up by an attacker by using a *rogue AP*).
Denial of Service (Dos)	Attacker prevents or prohibits the normal use or management of networks or network devices.
Eavesdropping	Attacker passively monitors network communications for data, including authentication credentials.
Evil Twin/Honeypot AP	Attacker sets up Honeypot AP with a default service set identifier (SSID, network name) hotspot SSID, or corporate SSID and observes many wireless clients connect to it and can then be initiate attacks on connected clients (e.g. stealing passwords by presenting a fake Facebook login page to clients over the mis-associated wireless connection.
Man-in-the-Middle	Attacker actively intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. Attacker can then masquerade as a legitimate party. In the context of a WLAN, a man-in-the-middle attack can be achieved through a *bogus* or *rogue AP*, which looks like an authorised AP to legitimate parties.
Masquerading	Attacker impersonates an authorised user and gains certain authorised privileges.
Message Modification	Attacker alters a legitimate message by deleting, adding to, changing or recording it.
Message Replay	Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.
Mis-configured AP	Attacker can take advantage of a potential security hole (open door) created by a mis-configured AP to launch an attack on the corporate network.
Rouge AP	Attacker can either plugged an unauthorised AP into the corporate network or use a computer (e.g. laptop) running software *fake AP* to provide wireless access to Wi-Fi clients within the range.
Rogue Clients	Attacker actively access an authorised cooperate wireless network via mis-configured AP (e.g. encryption turned off) or through an AP after compromising encryption/authentication.
Traffic Analysis	Attacker passively monitors transmissions to identify communication patterns and participants.

The applications of wireless technologies are found in many medical devices. The wireless communication system allows two way communication, information exchange and control of many different events. The wireless capability applies to both sensor and actuator systems and hence the range of risks is wide. In Table 2 a summary is made of potential adverse events that may occur if a wireless application fails to perform as intended (Hansen & Hansen, 2010, p. 15). In Table 3 a summary of potential threats against wireless systems is made, the related security requirement defined and possible security solutions specified (Ng, Sim & Tan, 2006, p. 141). The best-case scenario is that all possible security threats can be treated and will not materialise in a wireless medical network. The weaker case is that the possibility of adverse occurrences is reduced to a minor probability by mitigation of the causal factors. The residual risk in this instance should be such that the unintended variation can be managed within normal medical procedures and practices in such a way that the end user of the services has no negative consequences. With careful preparation and adequate protective measures wireless networks and wireless medical devices can deliver a better life experience and health opportunity. Our research highlights the trade-offs required for secure systems. A full assessment of the costs and benefits can reduce the potential of harm to an unremarkable amount that has no material impact on safety. However, reaching a point where a medical system is sufficiently robust and does not deliver adverse events requires comprehensive consideration of all probable controls. In the next section, we shall discuss the role of standards and standardisation in securing wireless medical systems.

Table 2. Potential adverse events in various implantable medical devices (Hansen & Hansen, 2010, p. 15)

Device	Adverse Events
Pacemaker, Implanted Cardiac Defibrillator (Mirowski et al., 1970); Ventricular Assist Device (Glenville & Ross, 1986)	Heart failure, Tachycardia, Bradycardia, Arrhythmia
Cochlear Implant	Deafness, Phantom sounds, Distraction/Confusion
Prosthetic Limb Control System (Velliste et al., 2008)	Injury, Damage to prosthetic limb, Inadvertent movement
Spinal Cord Simulator (Brindley et al., 1982)	Loss of pain relief, Inappropriate stimulation
Sacral Anterior Root Simulator (Brindley et al., 1982)	Infection from inability to void, Inappropriate stimulation
Retinal Prosthesis (Chow et al., 2004), Implanted Contact Lens, Intraocular Lens	Blindness, Phantom images, Distraction/Confusion
Implanted Infusion Pump	Inappropriate dosage/timing
Brain-Machine Interface and Other Neuroprosthesis (Santhanam et al., 2006; Song et al., 2009)	Loss of consciousness, Neural effects (Denning et al., 2009)
Responsive Neurostimulator and Other Deep Brain Simulator (Sun et al., 2008)	Inappropriate stimulation, Failure to stimulate
Implanted Monitor or Sensor	Incorrect readings
Implanted RFID Tag (Halamka et al., 2006)	Loss of privacy, Data leakage
Implanted Dynamic LED Tatto	Inappropriate display

Standards provide the opportunity for interoperability between medical systems and interoperability between the different medical devices. However, there is one substantial limitation with regard to the applications of wireless technologies in healthcare systems. The problem is the "the lack of interoperability among devices belonging to different vendors, even if they physically use the same wireless technology" (Delmastro, 2012, p. 1292). There is also a need for common data formats and transmission frequencies.

Table 3. Wireless sensor networks security threats, security requirements and possible solutions (Ng et al., 2006, p. 141)

Security Threats	Security Requirements	Possible Security Solutions
Unauthenticated or unauthorised access	Key establishment and trust setup	• Random key distribution • Public key cryptography
Message disclosure	Confidentiality and privacy	• Link/network layer encryption • Access control
Message modification	Integrity and authenticity	• Keyed secure hash function • Digital signature
Denial-of-service (DoS)	Availability	• Intrusion detection • Redundancy
Node capture and compromised node	Resilience to node compromise	• Inconsistency detection and node revocation • Tamper-proofing
Routing attacks	Secure routing	• Secure routing protocols
Intrusion and high-level security attacks	Secure group management, intrusion detection, secure data aggregation	• Secure group communication • Intrusion detection

There are numerous guidelines and standards related to medical healthcare technology. These guidelines and standards are created and embraced by international organizations, government agencies and professional or specialised organizations and societies (David & Judd, 2006). There are more than "20,000 individual standards and guidelines produced by 600 organizations and agencies from North America alone" (David & Judd, 2006, p. 75-14). Some of the standards address design and manufacturing practices for medical devices and related software although others apply to the safety and performance requirements for particular technologies (for instance, electrical and radiation safety standards). Likewise, standards are also required for the "coding and structure of clinical patient care data; the content of data sets for specific purposes; and electronic transmission of such data to integrate data efficiently across departmental systems within a hospital and data from the systems of other hospitals and healthcare providers" (Fitzmaurice, 2006, p. 41-42).

Table 4. Summarised top ten medical device challenges and possible solutions

Challenge	Possible Solution/Best Practice
1. Interfacing between devices and information systems	Provide appropriate education and training to users or technicians.
2. Maintaining computerized equipment and systems	Medical device manufacturers should validate their equipment with the most popular anti-virus and should provide clear instructions on how to install anti-virus program on particular devices.
3. Managing alarms	Clinical staff should be given education and training about the alarm setup, default settings and proper use of alarms in order to avoid the life and death of patients when alarms could not either be heard or ignored.
4. Maintaining and processing endoscopes	Users should be given proper education and training on how to clean, sterilize and maintain endoscopes as such devices are very sensitive and can be broken easily.
5. Broken connectors	Virtually all medical devices have some sort of connector and they can be difficult to replace. Furthermore, broken connectors are the most common cause of no problems founds (NPFs) when a clinician raises a concern about a device and then a technician checks it out. To prevent the issues related to broken connectors, setting a timer in connectors to remind if replacements are needed after a number of predefined connections has been reached.
6. Wireless management	The demand in wireless enabled medical devices for flexibility is raising one of the challenges in hospital/healthcare industry. Proper education and training should be given to users and IT personnel in order to maintain the devices.
7. Battery management	Healthcare facilities and patients/users of the medical devices should have efficient battery maintenance and replacement in their budgets as part of the preventive maintenance (PM) program. It is important to give proper training users and patients/users of the medical devices. Likewise, additional replacement battery packs and chargers should be given to mobile users of physiological monitors and defibrillators as batteries can easily be failed due to no power outlets available.
8. Problems with patient monitors (in-hospitals or at home, at work and around the community)	Users have to work with appropriate stakeholders, IT and clinicians to establish a risk management process that identifies vulnerabilities associated with patient monitoring systems and devices in order to mitigate all substantial risks.
9. Problems with dialysis equipment	It is essential to review the service schedule with clinicians and nurse managers responsible for dialysis service in advance of scheduled maintenance.
10. Managing the radiation dose from Computed Tomography (CT)	Radiation overdose and other dose errors is a top health technology hazard as a result of human error (wrongly administered radiation) or software-related errors. Users have to work with appropriate stakeholders, IT and clinicians to keep up the performance of such therapy systems and devices by regular maintenance.

The International Organisation for Standardization (ISO) and others are formulating standards for the safety of wireless medical systems. For example, specific standards include:

- Digital Imaging and Communications (DICOM)
- Health Level Seven International (HL7)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- European Union Data Protection Directive (1998)
- Medical Data Interchange (MEDIX) Standard
- IEEE P1073 Medical Information Bus (MIB)
- International Standard Organization/Institute of Electrical and Electronics Engineers (ISO/IEEE 11073 or X73), Personal Health Data (PHD).

The establishment of a robust system also requires control of many minor matters that are best associated with management policies, processes, procedures, and audit controls. Wireless connections now permeate all medical systems and devices and much risk can be treated by general management systems. In Table 4 the top ten challenges associated with managing medical devices are listed and risk mitigation strategies listed (Loughlin & Williams, 2011, pp. 99-103).

DISCUSSION

Wireless medical systems and devices offer measureable advantages for the delivery of medical services and end user flexibility. The vulnerability of wireless systems to attack, to mistakes and to technical problems has been reviewed in the background literature and requires risk management in order to maintain a safe environment. The degree to which vulnerabilities can escalate into serious events is amplified by the sensitivity of medical services. Events have implications for life quality, privacy and work effectiveness. Consequently, any residual risk has to be treated within the professional actions of a normal days work. However, published reports reviewed above related to the deployment of wireless communications and wireless medical devices in the healthcare industry show there have been a number of issues, events and challenges that have reduced the potential benefits. Prudent risk management has the ability to assure fewer adverse events and greater benefits. The numerous issues reviewed involved a lack of comprehensive coverage of wireless and mobile networks, reliability of wireless infrastructure, general limitations of handheld devices, medical usability of sensors and mobile devices, interference with other medical devices, privacy and security, misuse and malicious activities. The issues and challenges that require solution for effective service delivery can be grouped into five key areas; resources, electromagnetic spectrum, malicious attacks, standards and privacy.

Generally, wireless medical devices have limited resources (e.g. computational power, memory, and battery power). The resource constrains is one of the factors that can lead to compromised security and privacy of patients or device users. This also applies to the size of cryptographic algorithms that can be used. Similarly, the use of the electromagnetic spectrum for wireless communication introduces a capacity that is less than most wired networks. The nature of wireless devices allows the users of those devices to go anywhere at any time. As a result, there exists a potential issue related to the Electromagnetic Interference (EMI) among wireless medical devices employing the same ISM frequency band of 2.4GHz. For example, a Bluetooth enabled device can cause delay in transferring patient data and a packet loss up to 60% in a WPAN Electrocardiogram (ECG) monitor at very close range. When collaborative and non-collaborative actions are applied to mitigate the interference issues caused by the coexistence of WLAN and Bluetooth enabled devices the problem with interference is still unavoidable. Thus, there is a need for a strict monitoring and control of the spectrum usage in order to detect usage constantly, and to direct the choice of which technology to use. A similar service problem arises in many hospital buildings where heavy concrete structures and other obstacles can attenuate signals preventing the full use of bandwidth and EM resources.

The risk in medical systems of privacy breeches and inappropriate use of resources is high. A smaller but related risk is that of people hacking into the systems to achieve similar ends and impacts of an equal significance. Disruption to any medical service impacts patient health and life opportunities; whether it causes delays, extra costs, and inappropriate disclosures or affects the correct delivery of fluids or other services. In Table 1 the major threats to types of wireless networks and devices are summarised. In Table 2 the potential adverse events that may occur in some of the wireless enabled medical devices are also listed. These risks and consequences suggest that securing wireless networks and devices is crucial to patient safety at both a technical and managerial level. The security trade-off of these medical systems is the benefit of mobility and access. The medical services require protection from internal and external attacks while maintaining the best possible benefits for the patient and professionals from the technology. Insider attacks come from staff that may unintentionally or intentionally cause errors, loss of availability and integrity, financial loss and disclosure of sensitive information or the loss of physical assets. These risks may be mitigated by policies and managerial controls but they are difficult to eliminate. Table 4 summarises the top ten solutions for wireless medical device risk treatment.

The social and dynamic nature of human interaction introduces risk that cannot be zeroed without eliminating the very nature of the service being provided. External attacks are easier to defend against because standard IT protection mechanisms such as the firewalls or intrusion prevention systems and defence strategies can be applied to protect IT systems. Similarly, physical access to a hospital or healthcare organization can be controlled and unwanted access prevented. Again, the biggest threat is if social engineering techniques are applied and a malicious agent from outside of the system impersonates or seizes the identity of a beneficial agent then the system security is compromised. The context is the cost-benefit trade-off that reduces the effectiveness of perfect security solutions in proportion to user expectations. In a socially dynamic and socially engaged professional and community-based service, health has to engage and interface with many uncontrolled and deliberately uncontrollable variables. For example, a patient expects to be mobile and perhaps travel internationally when they have a pacemaker fitted to their heart. The health professionals in any country expect to have access to the pacemaker to provide the health services, when it is required. The risk is that with such open and potentially hopeful arrangements that the protective systems are not as secure as the current state of security knowledge for mobile devices allows. Few international standards cover interoperability and security of technologies in such circumstances. The problem then remains of accepting best intentions when mistakes and malicious activity may occur.

Standardisation has the greatest potential to treat security risks for wireless devices in health systems. Table 3 also adds techniques for mitigating threats and providing appropriate solutions. Managing security risks for wireless medical devices is an underdeveloped research area that requires further theorising. The issues arise because the solutions for best IT security may not appropriately fit the health services environment. The nature of health services requires high integrity in not only biological areas but also IT technical areas. The non-human IT objects interface and interact with humans and consequently require diverse responses to complex and high-risk human life situations. The health environment is constantly evolving to meet the requirements of services and the growing expectations of patients and professional staff. The performance of a doctor-nurse communication system, for example, has evolved from a simple telephone system, to text-based pagers and now into smart phone technologies. Along with the IT capability evolution so has the user expectations for performance, capability and effectiveness for health services evolved. The security of wireless medical devices is to go through similar transformations from the current situation and towards a better fit of protection and usage. Currently the ease of use for all stakeholders is traded against the perception of secure services and patient safety. Adverse events and growing user expectations will demand greater service integrity and benefits realisation.

CONCLUSION

The research and analysis suggest that the debate of securing wireless medical systems is not yet over. The literature shows that wireless systems are more vulnerable than wired systems to unplanned events and several key issues need to be solved. In the medical systems environment, medical devices and the service infrastructures require a minimal residual risk for potential disruption to the medical services. Managing the security risks is crucial to patient safety and system integrity. We are suggesting recognition of the requirements of socially engaged services in a medical environment and the subsequent cost of not being able to implement perfect IT security solutions, which leaves open the door for further research and IT security services development.

REFERENCES

Al, M., & Yoshigoe, K. (2011). Security and attacks in wireless sensor networks. In D. C. Kar & M. R. Syed (Eds.), *Network security, administration and management: advancing technology and practice* (pp. 183-216). United States of America: Information Science Reference, IGI Global.

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.

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

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

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

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.

Frankel, S., Eydt, B., Owens, L. & Scarfone, K. (2007). *Special Publication 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i – Recommendations of the National Institute of Standards and Technology*. Gaithersburg, Maryland: National Institute of Standards and Technology.

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.

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. *Proceedings of 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. *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

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.

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

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. *Proceedings of 7th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, Bucharest, Romania.

Paquette, A. (2011). Design of a pragmatic test lab for evaluating and testing wireless medical devices. *Proceedings of 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.

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

Radcliffe, J. (2011). Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System. *Proceedings of the Black Hat Security Conference (USA 2011)*, Las Vegas, United States of America.

Ren, Y., Pazzi, R., & 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. Proceedings of 2011 *1st Middle East Conference on Biomedical Engineering (MECBME)*, Sharjah, United Arab Emirates, 21-24 February 2011; pp. 283-286.

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.

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

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