A study of secure deployment of wireless technology in the Medical Fields

Nidal Turab
Assistant Professor, Faculty of IT, Al-Isra University, Jordan
nedalturab@ipu.edu.jo

ABSTRACT
Wireless Local Area Networks (WLANs) offer the organizations and users many benefits such as mobility, increased productivity and low cost of installation. This paper presents a proposal of deploying WLAN technology in hospitals. It starts with a brief review of the Health Level 7 (HL7), which is used to transfer medical records and data. In addition, a proposal of hospital network that makes use of a new Wi-Fi protocol, called Wi-Fi Protected Setup (WPS). The WPS is used to setup WLAN in easy and secure manner that meets the different requirements of hospitals, and the HL7 standard security requirements.

Keywords
Health Level (HL7), IEEE 802.11i, Temporal Key Integrity Protocol, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Wi-Fi Protected Setup (WPS).

1. INTRODUCTION
Security is the major weakness in the wireless technology, because there is no control over the communication channel (the wireless medium). In the wired networks each communication party has to have physical access to the communication media (i.e. wire). Wireless communication media is an open media where each user with a device equipped with wireless interface can use and share the airwave transmission medium with other users. The early WLANs were not designed for security, standards and methods are emerging for securing WLANs. Security protocols like WEP, WPA, and IEEE 802.11i are now good choices for encryption and authentication. These emerging security features must be implemented in order to assure a secure transmission of information on the wireless networks.

The Wi-Fi security protocol WPS is used for easy setup of a secure wireless network. WPS security strength comes from that security keys are generated randomly and the network name SSID is not broadcasted. On the other hand, the disadvantage of WPS is that all network devices must support it.

Health Level Seven (HL7) aims to provide standards for the exchange, management and integration of data that supports clinical patient care. There is a set of principles of the HL7 Version 3 [6]: Internationalization, interoperability between healthcare information systems, confidentiality of patient's information, non-repudiation and integrity. HL7 V3 defines standards for exchange, management and integration of data that is supposed to be collected and saved on the patient database [5].

1.1 Related work
Various researches had studied the deployment of WLAN in the medical field. Tia Gao, Dan Greenspan Wong [13] have developed a real-time application to allow remote monitor the patient, that system integrates different sensors such as: vital signs sensors and location sensors with ad-hoc networking, and web portal technology. In [7] Intel and CISCO developed WLAN Deployment Guide for Healthcare. More specifically, demonstrates the necessary steps of a WLAN deployment. The guide refers exclusively to Intel and Cisco technologies and equipment. Thaddeus FulfordJo and David Malan, introduced a wireless infrastructure to deploy in emergency medical care, that integrates low-power, wireless vital sign sensors, PDAs, and PC-class systems." [4]. Zachary Ochieng worked on a system to conduct surveys using mobile phones, to allow quick and easy transfer of data. The aim of the work was to benefit from the wireless technology to improve the access to health especially in poor locations. [15]. Theodore C. Chan and others [12]Discussed the application of new technologies in communications, wireless Internet and smart devices to improve the response of emergency medical services

This paper studies the application of the WLAN technology in the medical field and to propose a suitable WLAN solution for hospitals (independent of any vendor and using the latest security technologies). The proposed network is built on different levels of security using the new Wi-Fi security protocol WPS. It illustrates how our proposed network complies with the requirements of the HL7 standards. We have defined different types of wireless users in hospitals.

1.2. Wireless devices and patient safety in hospitals
Wireless technologies may have the impact in two areas: Electromagnetic Interference (EMI) with medical devices and electromagnetic radiation exposure, and the effects of radio frequency (RF) emissions on human health.

Wireless devices used in hospitals must meet safety and the *Electromagnetic Compatibility [EMC]* requirements. Electromagnetic compatibility means that any wireless device placed near a medical device should not cause harmful interference. The ISM-designated frequency bands are exempted

Copy Rights

from emission requirements in CISPR 11, because there are no radiation limitations for frequencies used in the WLAN [11].

The effects of Radio Frequency (RF) emissions on human health have been studied for many years. Studies [10] and [11] showed that there is a potential interference with some wireless portable devices, other than WLAN devices. As general precaution, but not required practically, it is recommended to keep the wireless devices about one meter distance from the hearing aids or pacemakers.

2. Proposal of a hospital network

The proposed network shown in fig.1

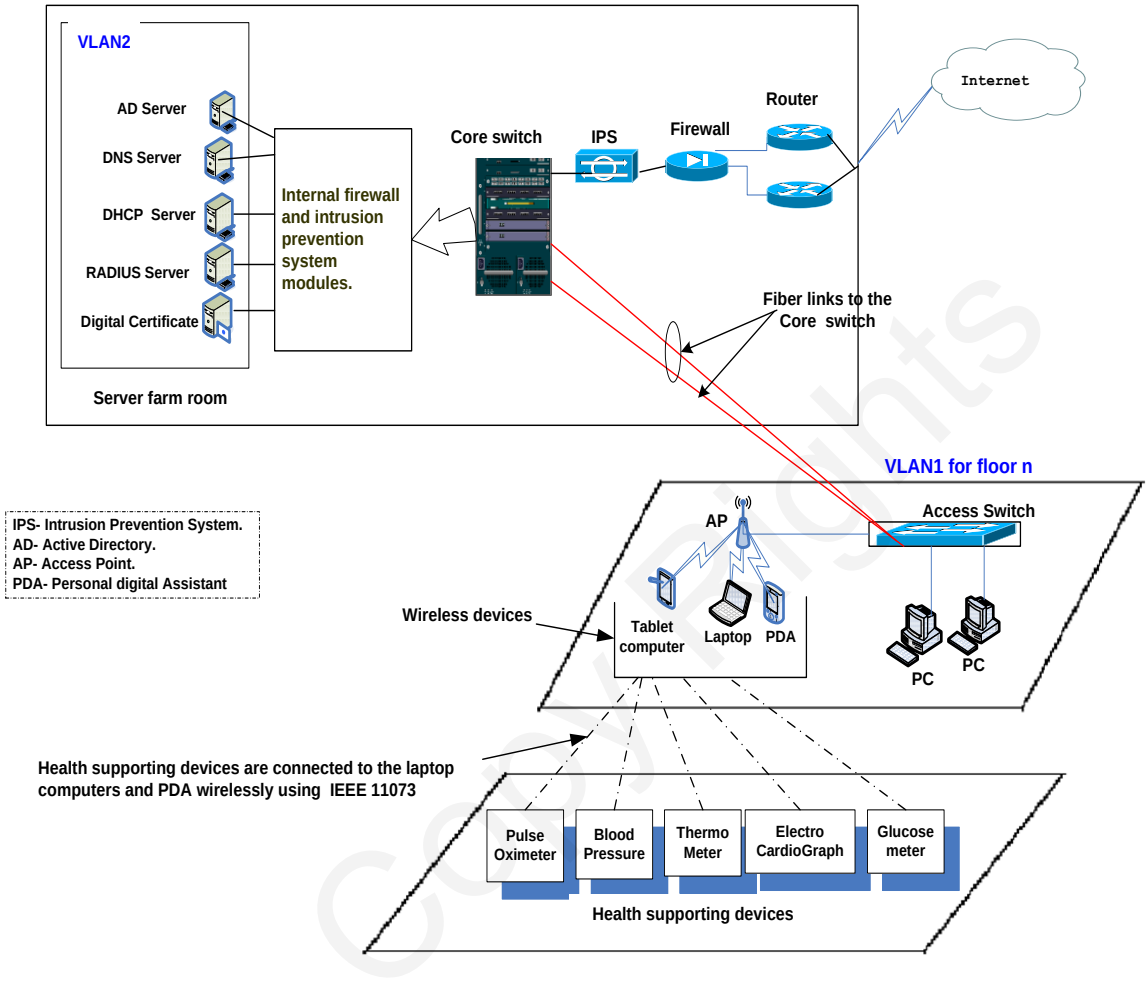

Fig. 1 Proposed hospital network architecture

a) The wired network part consists of the network devices and the servers that hold the hospital and patients applications.

b) The wireless network part contains wireless devices such as laptops and Personal Digital Assistants (PDAs) or even cellular phones that are equipped with wireless interfaces.

Layered security architecture for both the wired and wireless network; this layered security architecture is composed of the following components:

- Logical segmentation of the hospital's network into several Virtual Local Area Networks (VLANs)
- Multilayer core switch, which contains modules for QoS, firewall and intrusion prevention systems.
- External firewall and intrusion prevention system
- Different user privileges and access types; the privileges are assigned to the users according to their access type.

The wireless part of the network consists of wireless access points (APs) and the wireless devices, such as tablet computers, Personal Digital Assistant (PDA) and laptops. As shown in figure 1, typical personal health support devices (blood pressure monitors, weighing scales, electro cardiograph and pedometers)

collect information about a patient and transfer the information to the wireless device; the interaction between personal health supporting devices and the wireless devices is described in [9]. As in all WLAN environments, healthcare environments may consist of several access points in each floor, these access points are connected to dedicated wireless VLANs that can be at floor or department level.

For encryption and message integrity, the CBC-MAC of the AES encryption is used. For authentication, there are different scenarios (depending on the user access type, as we will discuss in the next section). In general, the authentication can be based on either IEEE 802.1x/EAP, that includes four-way handshake for the mutual authentication of the wireless client and the associated access point, or preshared key authentication using the Wi-Fi Protected Setup (WPS) to mitigate against forgery attacks. It should be noted that, IEEE 802.11 ad-hoc wireless connections are not recommended for hospital applications due to the security issues of ad hoc networks.

The medical staff can send patient data stored in their wireless mobile devices to one of the APs, which in turn, send it to the patient database stored on a server in the servers' farm on the wired network. This data could be either text or voice where voice recognition software on the server converts it to text

2.1 Users access types

There are different types of users in hospitals. For example, there is the medical staff, administrative staff, guest doctors, business guests and patients. Each user type requires a unique level of privileges. The access privileges of these users vary according to the nature of information they need to access.

Hospitals employee, medical staff and medical devices: can be assigned a VLAN that has access to the hospital's internal network (depending on the access privileges they were assigned) and to the Internet. Wireless communication from the wireless devices to the access points is secured by using IEEE 802.11i.

Guest access types include guest doctors, business guests and ordinary guests. It is necessary for guest devices to have separate Wi-Fi Protected Access Preshared Key (WPA-PSK). Re-keying can also be used to support guest access.

Guest doctors: also known as fellowship doctors, come from outside the hospital with their PDAs, and usually require access to the hospital's internal network and the patients' databases. A special VLAN is assigned to those physicians.

Business guests: are the technical engineers supporting medical equipments. They may require access to their company intranets over the Internet. VLAN for this type of users will be able to access their company networks using Virtual Private Networks (VPNs) over secure access to the Internet.

Ordinary guest users: consist of patients and their visitors who request Internet access during their stay in the hospital. Their access privilege should be strictly limited to Internet access only through a dedicated VLAN. In addition, the connection method to the WLAN should be simple and easy.

For guest doctors and business guest, the preshared key (PSK) of WPA is chosen in our configuration with AES encryption and CBC-MAC for message integrity.

To add mobile devices of these two guest users' types easily and securely to the WLAN, the Wi-Fi Protected Setup Protocol (WPS) [9] is used. The configuration of the wireless devices can be done by using out-of-band methods of WPS to transfer the WLAN configuration such as security parameters, the network name (SSID), radio channels and any other related parameters to the client's wireless device.

For ordinary guest users, the WPA-PSK with AES is used. With the in-band method configuration of the WPS is being used to join the wireless device to the WLAN. All the required information from the user is to enter the device password.

2.2 HL7 requirements and the proposed network architecture

Table 1 shows a summary of the HL7 message transport specifications. The table also includes a column to illustrate how our proposed network complies with the required HL7 message transport features.

The Domain Name Service (DNS) is required message transports in HL7, and is provided by the DNS server in the servers' farm. For authentication, there are two options: IEEE 802.1x/EAP-TLS authentication using digital certificates. The RADIUS and digital certificate servers provide the required components of the EAP-TLS. As stated earlier, this authentication can be used for permanent hospital employees and devices. For guest users the preshared key authentication is used with WPS, because WPS includes a modified version of EAP authentication and the Diffie-Hellman. This adds more security to the process of WLAN setup. WPS based setup prevents an adversary form launching password cracking attacks. Additionally, anti-reply protection is achieved in WPS by using the packet number. Finally, the authentication key used is 256 bits, which is higher than the one required by HL7. It is necessary to restrict configuration of the WLAN to a specific user account, to ensure that only authorized personnel can configure, manage and add new devices to the WLAN. Auditing can be done at several places either at the Active Directory server or at the RADIUS server. As shown in Table 1 below:

Feature	Availability in the proposed network as in figure 1
Routing	Yes (routing feature is provided by the core switch).
Reliable Messaging	Yes (our network is based on TCP/IP which is a reliable protocol stack).
Security	Layered security architecture.
Integrity	Yes (CBC-MAC and IEEE 802.1x authentication)
Confidentiality	Yes (encryption. authentication and data integrity and non-repudiation are basic parts of proposed network).
Non-Repudiation	Yes (digital certificate option is available).
Authorization	Yes (use privileges varies according to the user access type).
Authentication	Either IEEE 802.1x/EAP-TLS or preshared key authentication
Auditing	Yes (all users transactions are logged at the Active directory services and at the Registrar of the wireless segment).
Encryption	Yes (all wireless traffic is encrypted using CBC-MAC-AES)
DNS lookup	Yes (DNS lookup is included).
Minimum Public Key Length	1024 bits or higher
Minimum Session Key Length	256 bit.
In-order delivery of messages	Yes (TCP is a connection oriented protocol).

Table 1 HL7 required transport features

3. Conclusions

This paper is a proposal of a hospital network architecture that meets the requirements of HL7 message transport specifications and the different needs of users in a hospital.

Mobile devices (laptops, PDAs, cellular phones) of the medical staff cannot be only used to send patient data to the patient database stored on a server in the server farm, but also to transfer vital signs and measurements data (pulse oximeter, blood pressure, thermo meter cardiac strength, etc) from the patients' beds to doctors' mobile devices directly. Moreover, patients' data can be either text or voice. Voice recognition software on the server can convert the voice into text. The use of mobile devices gives the medical staff freedom to move and send data to the patient database from any location in the hospital.

REFERENCES

1. Alexandru Soceanu, Florica Moldoveanu, Andrei Földi "Future Computer Network Architecture An Overview", July 2007,University of Applied Sciences Regensburg.
2. "Architecture and Design of a Primary Wireless Network, 2006, URL: http://www.intel .com /it/pdf/architecture-design-of-pwn.pdf
3. "Enabling the integrated digital hospital", URL: http://www.intel.com/healthcare
4. Theodore C. Chan, William Griswold , Leslie Lenert "Information Technology and Emergency Medical Care during Disasters" http://www3.interscience.wiley.com/journal/119822403/abstract?CRETRY=1&SRETRY=0
5. Gunther Schadow "HL7 the data standard for biomedical informatics",2004, URL:http://www.openclinical.com/docs/ext/ conferences/cgp2004/ presentations/ schadow .pdf
6. "HL7 Announces ANSI Approval of Several Health Level Seven V3 Specifications", URL: http://xml.coverpages.org/ni2004-07-21-a.html
7. IEEE P11073-20601 Draft Standard for Health informatics- Personal health device communication, URL:http://ieeexplore.ieee.org/xpl/freeabs_all. jsp?tp=& isnumber=% 204410468&arnumber=4410469&punumber=4410467
8. Intel and Cisco "WLAN deployment guide for healthcare", March 2008 URL: http:// download.intel.com/healthcare/pdf/wlan_deployment_ guide.pdf
9. "Introducing Wi-Fi Protected Setup", Jan 2007 URL: www.wi-fi.org/files/ c_80_20070104_Introducing_Wi-fi_Protected_Setup.pdf
10. Jeffrey L. Tri, Jane M. Trusty "Potential for personal digital assistant interference with implantable cardiac devices," article Mayo Clinic Proceedings 79: 1527–1530,2004,URL:http://www.mayoclinicproceedings.com/inside.asp?AID=780 & UID=
11. Justin Boyle "Wireless technologies and patient safety in hospitals" Telemedicine and e-HEALTH ,Volume 12, Number 3, 2006
12. Thaddeus FulfordJones David Malan," CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", URL:www. ubimon.doc.ic.ac.uk/bsn/public/Malan-slides.pdf
13. Nidal Turab, Florica Moldoveanu, "The impact of various security mechanisms on the WLAN performance", Series C, Vol. 70, No. 4, 2008, ISSN:1454-234x, Scientific Bulletin of UPB.
14. Tia Gao, Dan Greenspan, Matt Welsh, Radford R. Juang, and Alex Alm " Vital Signs Monitoring and Patient Tracking Over a Wireless Network:, In Proceedings of the 27th Annual International Conference of the IEEE EMBS, Shanghai, September 2005.
15. World Health Organization "Electromagnetic fields and public health" May 2006, URL: http:// www.who.int/mediacentre/factsheets/fs304/en/
16. Zachary Ochieng "Health Services Benefit from Mobile Technology" http://www.cio.co.ke

Copy Rights