Consideration of Wireless 802.11x Security Encryption Protocols for use with Portable Medical Diagnostic Devices

Randall Bardwell – Mortara Instrument Inc.

Abstract: The use of wireless 802.1x networks is becoming a more viable option for use with portable medical electronic devices with the advent of higher bandwidth devices and the availability of wireless infrastructure. To provide data security on these wireless networks, a variety of security encryption protocols are utilized both on the server and client. The choice of security encryption can have far-reaching implications with regard to choices of diagnostic and data collection devices. This document discusses the various 802.11x wireless encryption methodologies as they relate to the medical environment specifically for the transmission of binary diagnostic information and their relevance with regard to implementation.

The burgeoning world of wireless clinical data communications: In the clinical world of wireless data transfer there is the reality of two data sets being propagated. One set of data encompasses the constant flow of clinical personnel communications data which is comprised of documents, spreadsheets, emails, and electronic charting data. The other set of information being transferred is more binary in nature and contains mostly diagnostic patient information in many digital forms ranging from blood pressure values to EKG's. The need to protect all of this data is a daunting task that is, in fact stipulated by the Health Portability and Administrative Act (HIPAA). While HIPAA does not specifically address the technical requirements of network security, it does require security to be implemented both with hardwire (IEEE 802.3) and wireless (802.11x) data networks.

Static 802.11x file transfer versus patient telemetry: Not to be discussed here, except for the sake of definition, exists also the technology of real-time patient telemetry. In this instance, a small transmitter acquires from 3 to 12 leads of real-time electrocardiographic data, digitizes it and transmits in one of the FCC allocated spectra. Interestingly, many of the same methodologies are starting to be adhered to in this technology space such as the concept of frequency-agile spread spectrum bi-directional packet communication. This technology is slowly working it's way into the fabric or wireless 802.11x networking but for now, we will consider only static file transfers as they typically will be transferred via the enterprise network.

The need for binary data network security: In the realm of consideration for wireless TCP/IP security, one must consider a couple of points. On one hand, if security was completely compromised on a network connected to a medical device transferring packets of binary textual, waveform, or image data, this data would have to be re-constructed utilizing the manufacturer's proprietary algorithm. On the other hand, if the device is utilizing the enterprise wireless network, one could not afford to compromise the integrity of the entire network on the premise that no one could or would care to decrypt and demodulate compressed binary medical data. Early on this was not a big consideration, as the concept has been, heretofore to segment the clinical network from the data network using a VPN. This had been the common practice to balance network loads, if nothing else. With the advent of packet identity technology such as Packeteer[1], the network can intelligently gate packets according to priority and thus one community network[2] can evolve, hence the need for robust security encryption technology.

Wireless Infrastructure affects product architecture: Diagnostic device infrastructure dictates to some extent the capabilities of the wireless client. Some encryption technologies such as EAP and Fortress Technologies utilize client-side encryption which requires an operating system environment in order to manage the decryption algorithms and to support the device drivers themselves. This innate need for an underlying operating system then mandates that the medical device itself provide the OS platform, otherwise an external embedded system platform is required. In some cases, the hardware requirements for these external OS based platforms can require substantial current requirements. In other cases, dedicated off-the-shelf wireless cards are required which, at face value from an engineering point of view, might seem to be expeditious but can in fact limit the technology capabilities of the device as you are then held to the market availability of PCMCIA or USB devices.

A real-time use model: Acquiring and collecting electrocardiograms (ECG's) works well in the model of wireless data transmission. The file sizes are very small, typically <25kB and the workflow in enhanced by the availability of the ECG order being transmitted directly to the electrocardiograph (ECG machine). When the order is generated by the electronic medical record system (EMR), it is transmitted to the ECG machine. The order is then accumulated on the ECG machine wirelessly. The ECG machine is then rolled to the room. When the order is selected, the patient demographic data is automatically entered into the record. The ECG is then recorded and transmitted to the EMR directly. Previously, the technician would have had to retrieve a paper order, enter the demographic information by hand and then roll the machine back down to a location to download the data. Wireless transmission saves time and effort at every point along the way by eliminating the need to "dock" the ECG machine to upload/download data.

Important obstacles in the engineering of the network: While proper wireless security can keep your network data safe, they can also keep non-compliant devices from functioning at all. Consider the story where a hospital had purchased 30 ECG machines at great cost only to find that the machines were incapable of utilizing the hospital's wireless encryption protocols. While most ECG machines will work with the simplest of encryption protocols, many will not work with mid-tier protocols such as WPA, and many more will not work with the higher level of security algorithms such as (L)EAP and Fortress. That having been said, it is good to evaluate the common landscape of encryption technologies:

Overview of relative security technology concepts:

RADIUS (Remote authentication dial-in user service) - The RADIUS server concept utilizes a network access device such as an access point in conjunction with a gatekeeper server with the function of administering log-in credentials to network access devices connected to a network access server (NAS).

WEP – Wired Equivalent Privacy - WEP is part of the IEEE 802.11 standard ratified in September 1999. It is the simplest form of wireless security. Typically implemented in 128 bit form, it affords the use of a static key set containing up to 64 characters. Shortcomings include the lack of key scheduling in order to thwart hacking attempts. Its has been demonstrated that WEP networks can be compromised in as little as three minutes[4], and thus it mostly being replaced with more robust encryption strategies.

WPA – Wi-Fi Protected Access – Implemented many of the 802.11i standards including the concept of Temporal Key Integrity Protocol or TKIP, which dynamically changes during the communications session. WPA is designed to be used with an authentication server such as RADIUS, however it can be implemented using "Pre-Shared Key" mode or PSK where the pass-phase is "pre-shared" with the user, hence the name. WPA2 implemented the remainder of the 802.11i standard including changing the Message Integrity Code (essentially the internal encryption algorithm) to the more secure CCMP (Counter Mode with Cipher Block Chaining Message Authentication Mode Protocol).

EAP – Extensible Authorization Protocol – An extension to PPP, EAP is an authentication framework comprising many different methodologies. EAP authenticates the user as well as the device through the use of user names and passwords. There are multiple vendor specifics variants such as (L)EAP – (Lightweight extensible authorization Protocol) is a security methodology devised by Cisco Systems employing mutual authentication and dynamic key management. EAP-TLS is considered to be one of the more secure implementations of EAP and is an open source protocol versus (L)EAP which is a proprietary offering, albeit being offered license free to vendors. EAP-TLS utilizes client-side certificates, or Public Key Infrastructure (PKI). This affords a very secure environment but is heavily dependant on client-side architecture.

FIPS-140-1, FIPS 140-2 - The National Institute of Standards and Technology is responsible for providing network security standards for use by the US Government. As part of their efforts, they specified a wireless encryption technology that went beyond the commercial standards and created a protocol that employed CCMP for message authentication but also the Skipjack algorithm message encryption (FIPS-185), a random number generator, and advanced dynamic key management algorithms. The Fortress Technologies[5] product became the first commercially available systems that is FIPS-140-1 and FIPS-140-2 compliant. This heavily client- side technology makes use of advanced RADIUS-like servers called gateways in order to implement the various encryption/decryption and authentication tasks. These extensive client requirements require the use of an embedded processor/OS in order to perform those numerous functions.

Summary:

It is important to first understand the wireless security technologies implemented in the healthcare environment and then to choose diagnostic devices that have utilized respective security methodologies that complement the security concept as a whole. While high-level security schemes may bode well for the whole of the enterprise, they may severely limit the vendors that may be considered for the data acquisition task.

On the other hand, vendors that have designed their clinical data acquisition devices with data communications security in mind will offer a more viable solution in the long run. Devices that offer multiple modes of security encryption will provide more secure pathways that will bode well for the sanctity of the enterprise network as well as the respect for HIPAA regulations. At the end of the day no matter what features a device might purport to offer, if the data cannot be safely propagated to it's destination, the device is more of a problem than a solution.

References:

1. Patient Monitoring in the Fast Lane
http://www.healthmgttech.com/archives/1205/1205patient_monitoring.htm

2. Infinity One Net System
http://www.innovations-report.com/html/reports/medicine_health/report-51774.html

3. Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison Wesley, 2003 (Updated in 2004), ISBN 0321136209

4. Feds hack wireless network in under three minutes
http://hardware.slashdot.org/article.pl?sid=05/04/05/1428250

5. Fortress Technologies
http://www.fortresstech.com/products_services/certificates_standards.asp