Securing Remote Obstetrics Monitoring Systems

Chiu C. Tan*
cctan@temple.edu
Department of Computer and Information Sciences, Temple University
Michael Korostelev
mike.k@temple.edu
Department of Electrical and Computer Engineering, Temple University
Li Bai
lbai@temple.edu
Department of Electrical and Computer Engineering, Temple University
Dimitrios S. Mastrogiannis
dimitrios.mastrogiannis@tuhs.temple.edu
Department of Obstetrics, Gynecology and Reproductive Sciences, Temple University School of Medicine
Jie Wu
jiewu@temple.edu
Department of Computer and Information Sciences, Temple University

Abstract

Many countries have experimented with deploying remote obstetrics monitoring systems as a means of improving the quality of prenatal care. The next generation of remote obstetrics monitoring systems incorporate off-the-shelf equipment like commercial smartphones into their design, to not only reduce the cost of the monitoring equipment, but also to allow for greater flexibility by letting the patient perform monitoring herself, in the comfort of her own home. In this paper, we analyzed the security protections of recently proposed monitoring systems and proposed recommendations to improve the security of these systems.

Keywords

Telemedicine, Fetal Monitoring, Security, HIPAA, Remote Obstetrics Monitoring

Introduction

Modern obstetrics care places a great importance on the assessment of fetal health, with electronic fetal monitoring being one of the most common obstetrics procedures performed in the United States. The frequency of fetal monitoring assessment will vary on the condition of the patient, with high risk patients requiring assessment once or twice per week. This places a high burden on patients who have to travel long distances to a hospital to receive access to specialized fetal care.

Advances in telecommunication technologies have made it possible to provide remote obstetrics monitoring service. In current remote obstetrics monitoring systems, the patient will visit a nearby clinic, rather than the hospital, for the monitoring service. The clinic will be equipped with the appropriate monitoring equipment, and the data collected will be transmitted to the hospital for diagnosis. This type of remote monitoring system is increasingly being deployed in the United States (Lowery, Bronstein, McGhee, Ott, Reece, & Mays, 2007), Australia (Chan, et al., 2000), and Europe (Fisk, et al., 1996).

In recent years, improvements in wireless communication and sensor technologies have led researchers to develop a more advanced form of telemedicine that can allow monitoring at home instead of the clinic (Jones, Gay, & Leijdekkers, 2010). While this is an active area of research, the majority of work in this area focused on the technical challenges (battery power management, data processing, etc.) in designing such a system, or user studies on evaluating the medical effectiveness of these systems. There has been relatively little research on exploring the security of such systems. Recently reported vulnerabilities on other types of medical devices, such as pacemakers (Halperin, et al., 2008) only serve as a reminder of the importance of ensuring the security of obstetrics monitoring systems.

Developing adequate security for remote obstetrics monitoring systems is important for two reasons. First, emerging remote monitoring systems are shifting away from hospital-grade monitoring equipment towards the use of consumer-grade equipment, such as smartphones, to build these monitoring systems. Consequently, remote obstetrics monitoring systems will now have to deal with the security vulnerabilities of such consumer-grade equipment. The second reason is the legal requirements that govern systems, like remote obstetrics monitoring systems, that deal with electronic health data. An example of legal requirements are the specific requirements laid forth by the Health Insurance Portability and Accountability Act, HIPAA.

In this paper, we will focus on emerging remote monitoring systems that allow for at-home monitoring with consumer-grade devices. We will compare the security of two recently proposed systems found in the academic literature against the HIPAA guidelines, and suggest possible modifications to enhance security. *We stress that the systems used in the analysis are prototype systems and may include additional security measures that are present, but not reported in the literature.*

Related Work

Remote obstetrics systems have been in operation for a number of years, and their medical and cost effectiveness are well studied (Kerner, Yogev, Belkin , Ben-Haroush , Zeevi , & Hod, 2004). A recent survey paper by Magann et. al. provides a good overview of this area (Magann , McKelvey, Hitt , Smith, Azam, & Lowery, 2001). However, there has been relatively little research done on the security of such systems.

There has been work done on the security of related systems. Body sensor networks (BSN) (Chen, Gonzalez, Vasilakos, Cao, & Leung, 2011) and mobile health (mHealth) (Avancha, Baxi, & Kotz, 2011) systems are a growing trend of healthcare monitoring research that is characterized by the use of inexpensive off-the-shelf components, like smartphones, to build health monitoring systems. Given the importance of security, there has been extensive research on BSN (Ng, Sim, & Tan, 2006) and mHealth security (Kotz, 2011). Unlike our work, most security research in this area addresses more general security threats, and do not focus on specific HIPAA requirements.

Background on Security Requirements

The general requirements for the HIPAA Security Rule are to provide protection for the confidentiality, integrity, and availability of data; defend against reasonably anticipated security or integrity threats; and protect against data disclosures not allowed under the HIPAA Privacy Rule. In this context, *confidentiality* refers to preventing unauthorized personnel from accessing data, *integrity* refers to protecting the data against unauthorized alterations, and *availability* refers to ensuring that data is accessible and usable to authorized personnel on demand. Next, we will present an overview of HIPAA security requirements, followed by describing the adversary model.

Summary of HIPAA requirements

We will mainly focus on the technical safeguards (*Section 164.312*) and some portions of the physical safeguards (*Section 164.310*) of the HIPAA Security Rule. The specific requirements are as follows. All except the last requirement fall under the technical safeguards. The last requirement belongs to the physical safeguards.

a) *Access control*. The system needs to regulate access to the data by authorized personnel or programs. Specific details include requiring the system to be able to identify and track a specific user, and have a means of allowing access to the data in an emergency. Also, the system may need to include a feature to perform encryption/decryption of the data and session control (e.g. automatically logging out the user after a period of inactivity).

b) *Audit control*. The system needs to implement a mechanism to record and examine the activities of the system.

c) *Integrity*. The system needs to incorporate mechanisms to both protect the stored data, as well verify that the stored data has not been tampered with.

d) *Person/Entity authentication*. This requires the system to verify that the identity of the entity accessing the data is correct. In other words, authentication allows a system that restricts access to a particular doctor to actually verify which doctor is accessing the data.

e) *Transmission security*. This requires the system to prevent unauthorized access of the data during transmission over the network. This includes encryption of the data during transit, as well as methods to determine that the data has not been modified during transit.

f) *Device and media controls*. This requires procedures to ensure that the data be safely deleted when the user is no longer using the system, or when the system is re-issued to a different user.

We define an adversary as one whose goal is to violate one or more components described above. We assume that the adversary has knowledge of the monitoring system, e.g., information such as communication protocols, schedule of data transmission, and so on. We also assume that the adversary will have access to any hardware necessary to communicate with the monitoring system. Thus, if some specialized hardware is used to communicate with the monitoring system, the adversary is assumed to have access to that hardware as well. Our analysis excludes denial-of-service attacks, such as wireless jamming which can prevent any communications between the monitoring system and the hospital servers.

Traditional systems	**Emerging systems**
• Treatment occurs in clinic	• Treatment occurs at home
• Medically trained staff present	• No medical staff present
• Equipment used is medical grade hardware	• Equipment used is off-the-shelf hardware

Table 1: Summary of differences between traditional and emerging remote obstetrics monitoring systems.

For convenience, we assume that all the data is to be stored on the hospital's servers. We restrict our discussion to attacks on the monitoring system itself, and not on the hospital information technology infrastructure. Once the data is stored in the hospital's database system, the data is considered secured. The hospital thus can be considered a trusted party.

Remote Obstetrics Monitoring Systems

We can divide remote obstetrics monitoring systems into two categories. The first category includes *traditional* systems where standard hospital monitoring equipment, like a fetal cardiotograph are installed in an off-site location such as a clinic (Lieto, et al., 2008). Trained medical professionals operating the cardiotograph will treat the patient. The data collected by the cardiotograph will then be transmitted to the hospital where specialized obstetricians will interpret and diagnose the data. Such a system can allow patients, especially those who are living in remote areas, access to a high level of care while reducing the financial cost. This is accomplished, in part, by leveraging the existing general care network to perform the monitoring with specialized diagnosis being performed in a centralized location. Traditional monitoring systems are well studied, and their effectiveness well documented (Kosa, et al., 2008).

The second category of remote obstetrics monitoring systems are emerging systems where off-the-shelf equipment like smartphones modified for fetal monitoring are used, in lieu of a more conventional fetal cardiotograph (Shim, Lee, Hwang, Yoon, & Yoon, 2009). For home-based monitoring systems, the patient herself will be operating the monitoring equipment (Lee, Masek, Lam, & Tan, 2009). Similar to the traditional system, the data is transmitted to the hospital to be analyzed by the obstetrician. Emerging systems can further reduce costs by eliminating the need for a medical professional to administer the monitoring. Off-the-shelf monitoring equipment is also cheaper than standard monitoring equipment. Similar to traditional monitoring, home-based data will be transmitted to a remote hospital, where specialized medical staff will interpret the results. While both traditional and emerging systems allow for remote obstetrics monitoring, there are key differences with significant security implications. Table 1 summarizes the differences.

The first difference is that the monitoring is no longer restricted to a clinic, but to the user's home. By performing monitoring at the clinic, system designers can assume a certain (higher) level of security protections. Off-site clinics are already likely to have in place, for instance, procedures and mechanisms to authenticate the patient, regulate equipment access, secure databases, up-to-date computers, and so on. However, these same assumptions cannot be made in a home environment, which in turn complicates the system design. For example, in a traditional system, the monitoring device may not need to be password-protected, since the clinic may very well have its own procedures to manage the problem. In the emerging system, some password protection mechanism, together with the corresponding password management, will need to be in place.

In home-based monitoring, there are no medical professionals at hand to operate the monitoring device. As a result, emerging systems may require a redesign of the user interface to provide adequate feedback, so that the user is able to operate the device correctly. Furthermore, emerging systems may have to manage the situation where the monitoring device detects an emergency situation, since there is no medical staff readily available to help the user.

Finally, emerging systems make extensive use of commercial smartphones as a means of coordinating the sensors, collecting the data, and transmitting it to the hospital servers. Unlike dedicated medical devices used in traditional systems, these smartphones are multi-purpose devices, which are open to greater security risks. For instance, the user may accidentally introduce a virus into the smartphone by downloading an app, which may in turn compromise the security of the monitoring system. This type of security threat is minimized in traditional monitoring systems, which are dedicated to a particular task.

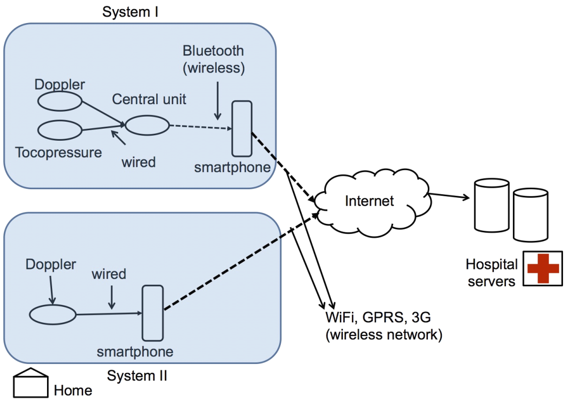

Figure 1. Architecture of System I (top) and System II (bottom)

Emerging Systems in Detail

To better analyze the security implications of emerging obstetrics monitoring systems, we focus on two recently proposed systems. We stress that both systems are still in the proof-of-concept stage, and thus any security features (or lack of), should not be interpreted as flaws in the systems. Furthermore, security regulations like HIPAA may not even be applicable, for instance, when the system is to be deployed outside the United States.

System I. This is a system proposed by Roham et. al. (Roham, Saldivar, Raghavan, Zurcher, Mack, & Mehregany, 2011). The main components of the system are (1) monitoring devices, (2) central unit, (3) gateway device. Figure 1 illustrates the system architecture. There are two types of monitoring devices, a toco pressure sensor and an ultrasound Doppler heartbeat detector. The monitoring devices are connected to the central unit via a wired connection. The central unit does some data processing on the heartbeat data to filter out errors, and also forwards the collected data to the gateway device. The central unit and the gateway device use a wireless communication channel in the form of Bluetooth. The gateway device is an Android smartphone. The gateway device will use WiFi, GPRS, Edge or a 3G wireless network to transmit the sensed data back to the hospital's server. The data transmission is performed using secure file transfer protocol (SFTP), which means that the gateway does not depend on the wireless network to provide security.

System II. This is a system proposed by Lee et. al (Lee, Masek, Lam, & Tan, 2009). The main components are (1) a handheld Doppler device and (2) a smartphone. The Doppler device is connected to the smartphone using an audio cable. The smartphone is a TyTN II phone running Windows Mobile OS. The smartphone processes the data and transmits it back to the hospital server using GSM or GPRS. This system incorporates a feedback design that informs the patient when the data has completed its transmission to the hospital servers. Once the data is successfully transmitted, the hospital servers will send an electronic message to the medical professional that new data is available for diagnosis. A separate publication by the same group notes that HTTPS protocol is used to encrypt the data during transmission to the servers. While this system does not incorporate a toco pressure sensor, the system allows the patient to manually input into the smartphone when there is any fetal activity. This input is issued a timestamp, and later matched with the fetal heartbeat information.

	System I	**System II**
Access control	Partial	Partial
Audit control	No	No
Integrity protection	Partial	Yes
Authentication	Partial	Partial
Transmission security	Yes	Yes
Device/Media controls	Unknown*	Unknown*

Table 2. Summary of security analysis. The "" indicates that requirement can probably be incorporated easily if not presently incorporated.*

Security Analysis

Next, we will analyze the security features for Systems I and II, based on the system description. For meaningful analysis, we will assume that conventional security features common to most smartphones are present, regardless of whether it was mentioned in the original papers. Table 2 summarizes the results.

Access control requirement

In System I, the data from the sensors are transmitted to the smartphone from the central unit using Bluetooth. The security of Bluetooth ensures that the data reaches the smartphone securely. Since most smartphones have a password feature, we can assume that only authorized personnel can have access to the password, and thus the data. Both smartphones appear to support a removable microSD card for larger storage capacity. Assuming that the data is stored in the microSD card, the card can be removed to access the contents in an emergency situation. An auto-log off feature can be easily added if necessary. In System II, the sensors are directly plugged into the smartphone, and the same features of the smartphone, can be used to provide access control, as in System I.

However, neither System I nor II support encryption of the data while it is inside the smartphone. An adversary with physical access to the smartphone can remove the microSD card to access the data. An adversary-controlled malicious app, which the user unknowingly installed on the smartphone can also potentially have access to the stored data.

Audit control requirement

Both systems perform some data processing on the data collected by the Doppler device. However, neither system appears to implement any system to record the operations of the sensing device or the smartphone. As such, it does not appear to be possible to perform any diagnosis of the system activities.

Integrity requirement

System I uses SFTP to transfer the data from the phone to the hospital's servers. SFTP provides integrity protection during the data transfer. However, there does not appear to be any notification in the event of network failure during the data transfer process from the smartphone to the servers. This can potentially create the following vulnerability.

System I allows the smartphone to choose the best wireless networks (WiFi, GPRS, 3G, and so on) to transmit the data. In an environment with poor network connectivity, different portions of the data could be uploaded using different wireless networks to the server. This might lead to a violation of integrity protection when, for instance, all but the last portion of the data was never uploaded successfully. The integrity protection offered by SFTP only applies to the data transmitted *within* each SFTP session, and the smartphone will have to create a new SFTP session each time it switches to a different wireless network. As a result, the doctor’s diagnosis on the data from the hospital's server may be incomplete, thus violating integrity.

System II uses HTTPS to transfer data from the phone to the hospital servers. HTTPS is built on top of transport layer security (TLC) which provides integrity protection.

System II incorporates a user feedback mechanism that informs the user when the data has been successfully uploaded, and then informs the medical personnel that the data transfer is completed.

In the same scenario as before, the user is aware that the data on the hospital's server is incomplete and can try to upload the data again later, or inform the hospital, so as to prevent the obstetrician from using incomplete data for diagnosis. This will prevent medical personnel from diagnosis with incomplete information.

Person/Entity authentication requirement

Both systems can use the password feature of the smartphone to satisfy person authentication requirement. However, neither system appears to perform any entity authentication on either the smartphone or the sensing devices, e.g. Doppler ultrasound. In other words, the hospital does not know whether the data is collected using a valid device or not.

The use of an invalid device can cause multiple problems. A wrongly calibrated device may be used for the monitoring, and thus, may result in incorrect data being used for diagnosis. An unauthorized smartphone will lack the necessary security protections that the hospital requires, such as the inability to install third-party applications. As a result, a user may transmit their data to the hospital using an unauthorized smartphone that may have be tampered with by the adversary. It is worth noting that requiring the user to enter a password to access the smartphone only authenticates the user to the phone. We cannot assume that the phone is authorized, since the adversary can let the smartphone simply allow any password to be acceptable.

Transmission security requirement

Both Systems I and II use standard secure data transmission protocols to transmit data from the device to the hospital. Therefore, both systems provide transmission security.

Device/Media controls requirement

Neither system details the procedures for device and media controls. However, since both systems use removable storage in the form of a microSD card, existing hospital policies on device and media controls can be extended to meet this requirement.

Security Recommendations

From the security analysis, we see that emerging systems tend to have good transmission security protections, but remain vulnerable to other types of attacks. The following are some recommendations that can help emerging monitoring systems better meet HIPAA Security Rule requirements

Restrict Smartphone Apps

One reason for the popularity of smartphones is the existence of apps, which are small, yet powerful, programs running in the phone. The majority of these apps are free or very inexpensive, costing only a few dollars. Popular apps include games, movies, navigation, and so on.

However, a recent study on 1,400 iPhone apps have found that more than 50% of the apps reveal the specific device ID of the phone. While there is no direct link between the device ID and the user's identity, the device ID can be used to track the user over time. (Egele, Kruegel, Kirda, & Vigna, 2011). Another study focusing on Android apps showed similar privacy problems, with half of the apps surveyed revealing the phone's location, and one third transmitting the device ID (Enck, et al., 2010).

Given the privacy risks poised by smartphone apps, one option is to modify the smartphone OS to remove existing apps from the phone, as well as disabling the option for the user to install new apps. However, this approach may only be practical if the phone is supplied by the hospital as part of the monitoring kit.

There is a trend towards "Bring Your Own Device" (BYOD) in hospitals, as people are more comfortable with using their own device, rather than be trained to use a specific hospital provided device. Recent developments in virtualization have made it possible for a smartphone to support different virtual machines (Barr, et al., 2010). As such, a special "fetal monitoring" VM can be loaded to run in the smartphone while the patient is undergoing the monitoring process. This specific VM can be configured as necessary, to process the sensor data and provide the security protections. The patient can switch back to his regular smartphone OS after the monitoring is over. (Fetal monitoring is only performed for a relatively short period of time, approximately 20 to 40 minutes.) This may become the preferred approach for smartphone-based monitoring systems because the same phone can be loaded with different VMs for different types of monitoring applications, while still allowing the patient the freedom to use his own device the rest of the time.

Performing device authentication

As outlined earlier, both user *and* device authentication are necessary to provide integrity protections. Having the user enter a password only authenticates the user as a valid patient. It does not indicate that the device is authenticated.

Ideally, all components of the monitoring system, e.g. the Doppler ultrasound, the tocopressure sensor, central unit, and the smartphone itself, should be authenticated to make sure that all components are legitimate. However, since only the smartphone is a general purpose computing device, it makes the smartphone more vulnerable to adversary compromise, as compared to the rest of the components.

This can be accomplished by maintaining certificates identifying each particular smartphone, and then installing the correct certificate onto the phone. Certain types of smartphones already support this option, where it is sometimes used for phones that need to be configured for secure network access like a virtual private network (VPN).

Improving user authentication

The descriptions from Systems I and II omit details on how a user will authenticate with the phone. However, it is reasonable to assume that the built-in authentication method was used to perform the authentication. Note that, since the smartphone is the most powerful device in the monitoring system, it will also likely serve as the gateway for authenticating the patient to the hospital system. In other words, a user authentication on the smartphone that allows unauthorized users to use the monitoring system will potentially lead to health data from the unauthorized users to be added to the medical records of the patient. This is the reason why user authentication on the phone is especially crucial.

The most common built-in authentication for the smartphone is where the user has to enter either a PIN or password to access the phone (Funell, Clarke, & Karatzouni, 2008). Putting it within the hospital context, we can have each patient be issued with a unique password for the phone when they initially obtain the fetal monitoring equipment from the hospitals. However, studies on user attitudes towards traditional PIN or password authentication have revealed users' dissatisfaction. One study indicated that 30% of users considered using a PIN inconvenient, and only 25% of users believed that the PIN provided adequate security protections (Clarke & Furnell, 2005). More importantly, 38% of users had to contact their phone providers to unblock their phones after they had locked up their phone from entering the incorrect PIN multiple times. This suggests that using a PIN or password to secure remote obstetrics monitoring systems may not be ideal. Adequate security protection requires the phones to be issued with strong passwords, which are often longer and more difficult to remember. This will, in turn, increase the likelihood that users will either forget, enter an incorrect value, or simply write the password down, reducing the efficiency of the security protections.

There are two alternatives to password or PIN-based user authentication. The first is *biometrics-based* authentication. In this type of authentication, some unique physical feature is used. The smartphone will collect and process a signature of this physical feature, and will unlock the phone only if the monitored features match the authorized ones. Since biometrics are unique to each patient, unauthorized users that attempt to access the monitoring system will have different biometric features than the authorized patient, and thus be refused access. While there are many different types of biometrics, a promising biometric for remote obstetrics monitoring is the one based on using electrocardiography (ECG) signals to distinguish patients. Researchers have determined that ECG can be used to distinguish between individuals (Biel, Pettersson, Philipson, & Wide, 2001), and subsequently have proposed authentication protocols based on this observation (Sriram, Shin, Choudhury, & Kotz, 2009). The advantage of using ECG as an authentication method for a remote obstetrics monitoring system is that the necessary hardware to measure the ECG may already be present in the monitoring system. The drawback for using ECG for authentication is that it is a relatively immature technology. All of the existing ECG authentication systems we are aware of are research prototypes, not mainstream products. In the short term, this may mean that supporting ECG-based authentication will be a less attractive option for hospitals.

The other alternative to passwords and PINs are *token-based* authentication methods. In this approach, the patient is issued with a hardware token which can take the form of a key chain, watch strap, or ID card. A secret value, unique to each patient, is stored in the hardware token. The patient authenticates herself with the smartphone by placing the hardware token near the phone. The token and the phone will interact using Near Field Communications (NFC) wireless communications to complete the authentication process. NFC hardware is already available on Android smartphones. Figure 2 shows some prototype hardware tokens we experimented with in our own remote monitoring system design.

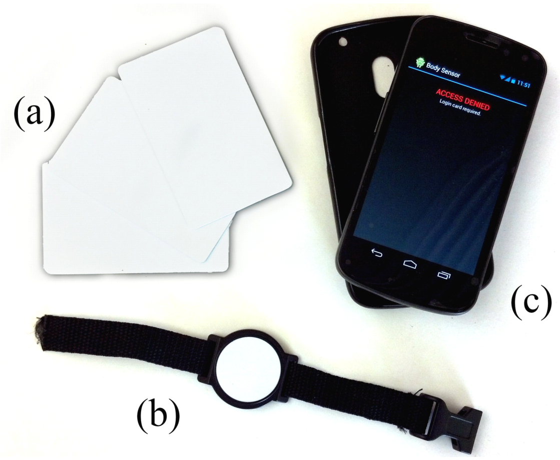

Figure 2. Examples of hardware tokens used for authentication. (a) is a token in the form of a user ID card. (b) is a token in the form of a wristwatch. (c) is the NFC enabled smartphone.

Token-based authentication is an improvement over passwords because the patient does not need to remember the password or PIN to authenticate herself. Unlike biometric-based authentication, however, the patient has to keep the hardware token safe. An unauthorized user with access to the hardware token will gain access to the monitoring system. However, this is unlikely to be difficult for a patient to do. A hardware token, for instance, in the form of a ID card can be protected just like a regular credit card.

There are several advantages of using NFC hardware tokens to authenticate the patient. First, the NFC tokens do not require a battery to function. This makes them more reliable, since we do not have to worry about replacing batteries. NFC tokens only function when in the presence of an active counterpart (reader/writer). The NFC tokens operate using three embedded hardware resources. The RF Interface serves as the communications and power system aboard the card by acquiring both energy and information in a fashion similar to the crystal radio. The energy is used to power devices within the Digital Control Unit and EEPROM to effectively manipulate digitized information. Second, each NFC token is able to store and transmit additional amounts of data, in addition to authentication. For instance, the Mifare 4K card has up to 4KB of storage space in which to store additional patient information. This provides the system developer greater flexibility to include additional information (e.g. ultrasonic amplification levels for obese patients) into the token as necessary. For instance, the system designer can include information such as the number of medical sensors that the phone is supposed to connect with, and their calibration information, into the token. When the patient authenticates herself to the phone, the phone will also receive this information, and perform a diagnostic check to make sure that the correct sensors are present. If there is a missing device that is not included in the monitoring process, the smartphone can notify the patient to place all devices into the monitoring process. Finally, NFC hardware tokens are a relatively mature technology, and are already being used in hospitals. This makes it easier for hospitals to support monitoring systems using this type of technology.

Improving the user feedback process

Another recommendation is to improve the user feedback process in both the data transfer process and the data collection process. Emerging monitoring systems rely on wireless networks like WiFi or cellular networks to transmit data from the home to the hospital. However, the wireless networks may not always have sufficient bandwidth to support remote monitoring, especially when a streaming video needs to be uploaded to the hospital servers. A normal diagnostic video for example, will require between 768 KB/s to 10 MB/s, depending on the quality of the video (Niyato, Hossain, & Diamond, 2007). Emerging 4G wireless networking technologies such as WiMAX will have higher bandwidth and provide better quality-of-service (QoS) support, factors which can potentially address this problem. However, we cannot simply rely on 4G networks alone, since there will inevitably be areas of unreliable or unavailable wireless coverage, which will prevent the collected data to be uploaded in a timely fashion to the hospital for diagnosis.

One improvement is to incorporate a patient feedback process, like that implemented in System II, into the monitoring system. Allowing the patient to be aware of whether the data has successfully been uploaded or not will allow the patient the ability to undertake additional action, e.g. send data via wired connection, or drive down to the clinic to upload the data, if necessary.

As an additional safety feature, the remote monitoring systems can also consider developing an automatic warning to alert the patient in certain dangerous situations. One limitation of remote monitoring systems is that it is unclear to the patient whether the data has already been analyzed by a medical professional. Including an automatic warning service into the remote monitoring system will help address this problem. Prior to deploying the monitoring system, the patient's doctor can pre-set certain values into the smartphone. These values represent warnings that the patient should seek medical attention directly. As the data is collected from the sensors, the smartphone will verify the collected data against the pre-set values, and alert the patient as necessary. This warning function will help improve the safety of the remote monitoring system.

Encrypting data at rest

For remote monitoring systems that transmit the data to the hospital immediately after collection, it might be unnecessary to encrypt the data captured in the phone, assuming that the data is to be transmitted to the hospital servers almost immediately after collection, and adequate mechanisms are in place to notify the user of a successful or unsuccessful transmission. The reason is that the data can be deleted after the transmission has been completed, reducing the risk of data being exposed in the event that the phone is misplaced. Avoiding encryption on the phone itself also has two additional benefits. First, it simplifies the overall system design, since the hospital can avoid having to set up an additional key management system to manage the keys. Second, it becomes easier to handle emergency situations where the data needs to be accessed immediately. Without encryption, we can simply remove the microSD card to read the data, but encrypting the data will require additional procedures to decrypt the data, in the case of needing emergency access to it.

However, since guaranteed transmission is not possible, the data may have to remain in the phone for long periods of time before it can be safely deleted. As such, it is advisable to develop the monitoring system to encrypt all the data stored in the phone, even if the system was designed to transmit all data immediately after collection. Here, it is worth stressing that the monitoring system cannot rely on user-smartphone authentication to protect the data. While the user-smartphone authentication can be set up to prevent an unauthorized user from accessing the phone, it does not necessarily protect the data stored in the phone's removable media. Using encryption helps satisfy the HIPAA "safe harbor" provisions for personal health information.

Conclusion

Emerging remote obstetrics monitoring systems have the potential to lower the cost of providing quality obstetrics care by using commercial components. However, this also comes with additional security risks that are absent from traditional remote monitoring systems. In this paper, our analysis of two recent system designs suggests that additional security protections besides simply securing the data transmission is necessary to meet HIPAA requirements.

Acknowledgements

This research was supported in part by NSF grants ECCS 1241461,CNS-1156574,CNS 1138963, ECCS1128209, CNS 1065444, and CCF 1028167, as well as by the Formula Fund from the State of Pennsylvania.

References

Avancha, S., Baxi, A., & Kotz, D. (2011). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys* .

Barr, K., Bungale, P., Deasy, S., Gyuris, V., Hung, P., Newell, C., et al. (2010). The VMware mobile virtualization platform: is that a hypervisor in your pocket? *SIGOPS Operating System Review* .

Biel, L., Pettersson, O., Philipson, L., & Wide, P. (2001). ECG Analysis: A New Approach in Human Identification. *IEEE Transcations on Instrumentation and Measurements* , 808-812.

Chan, F., Soong, B., Lessing, K., Watson, D., Cincotta, R., Baker, S., et al. (2000). Clinical value of real-time tertiary fetal ultrasound consultation by telemedicine: preliminary evaluation. *Telemedicine journal : the official journal of the American Telemedicine Association* , 237-242.

Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. (2011). Body area networks: A survey. *Mobile Network Applications,* , 171-193.

Clarke, N., & Furnell, S. (2005). Authentication of Users on Mobile Telephones: A Survey of Attutudes and Practices. *Computers and Security* , 519-527.

Egele, M., Kruegel, C., Kirda, E., & Vigna, G. (2011). PiOS: Detecting privacy leaks in iOS applications. *Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS).*

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., et al. (2010). TaintDroid: An Information-Flow Tracking System for Realtime PrivacyMonitoring on Smartphones. *9th USENIX Symposium on Operating Systems Design and Implementation (OSDI).*

Fisk, N., Sepulveda, W., Drysdale, K., Ridley, D., Garner, P., Bower, S., et al. (1996). Fetal telemedicine: six month pilot of real-time ultrasound and video consultation between the Isle of Wight and London. *British journal of obstetrics and gynaecology* , 1092-1095.

Funell, S., Clarke, N., & Karatzouni, S. (2008). Beyond the PIN: Enhancing User Authentication for Mobile Devices. *Computer Security and Fraud* , 12-17.

Halperin, D., Heydt-Benjamin, T., Ransford, B., Clark, S., Defend, B., Morgan, W., et al. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. *IEEE Symposium on Security and Privacy.* Washington, DC: IEEE.

Jones, V., Gay, V., & Leijdekkers, P. (2010). Body Sensor Networks for Mobile Health Monitoring: Experience in Europe and Australia. *Proceedings of the Fourth International Conference on Digital Society* (pp. 204-209). Washington, DC: IEEE.

Kerner, R., Yogev, Y., Belkin , A., Ben-Haroush , A., Zeevi , B., & Hod, M. (2004). Maternal self-administered fetal heart rate monitoring and transmission from home in high-risk pregnancies. *International Journal of Gynecology and Obstetrics* .

Kosa, E., Horvath, C., Kersner, N., Kadar, K., Kovacs, F., Torok, M., et al. (2008). Experiences with fetal phonocardiographic telemonitoring and future possibilities. *International Conference of Engineering in Medicine and Biology Society.* IEEE.

Kotz, D. (2011). A threat taxonomy for mHealth privacy. *Workshop on Networked Healthcare Technology* .

Lee, C., Masek, M., Lam, C., & Tan, K. (2009). Advances in fetal heart rate monitoring using smart phones. *International Symposium on Communications and Information Technology.*

Lieto, A., Falco, M., Campanile, M., Torok, M., Gabor, S., Scaramellino, M., et al. (2008). Regional and international prenatal telemedicine network for computerized antepartum cardiotocography. *Telemedicine and e-Health* .

Lowery, C., Bronstein, J., McGhee, J., Ott, R., Reece, A., & Mays, G. (2007). ANGELS and University of Arkansas for Medical Sciences paradigm for distant obstetrical care delivery. *American journal of obstetrics and gynecology* .

Magann , E., McKelvey, S., Hitt , W., Smith, M., Azam, G., & Lowery, C. (2001). The use of telemedicine in obstetrics: a review of the literature. *Obstetrics Gynecology Survey* , 170-178.

Ng, H., Sim, M., & Tan, C. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal* , 138-144.

Niyato, D., Hossain, E., & Diamond, J. (2007). IEEE 802.16/WiMAX-based Broadband Wireless Access and its Application for Telemedicine/E-Health services. *IEEE Wireless Communications* , 72-83.

Roham, M., Saldivar, E., Raghavan, S., Zurcher, M., Mack, J., & Mehregany, M. (2011). A mobile wearable wireless fetal heart monitoring system . *International Symposium on Medical Information Communication Technology* .

Shim, H., Lee, J., Hwang, S., Yoon, H., & Yoon, Y. (2009). Development of heart rate monitoring for mobile telemedicine using smartphone. *International Conference on Biomedical Engineering.* IEEE.

Sriram, J., Shin, M., Choudhury, T., & Kotz, D. (2009). Activity-aware ECG-based Patient Authentication for Remote Health Monitoring. *International Conference on Multimodal Interfaces* (pp. 297-304). New York: ACM.