A Light Review of Data Security and Privacy Approaches Applicable to E-Health Systems

Ninad Desai, Hamid Shahnasser
School of Engineering
San Francisco State University
ninad.desai24@gmail.com

ABSTRACT

While e-health sounds as a promising future for healthcare and medicine, it still is far from being integrated into our day-to-day lives. While interoperability and data link reliability are important issues that need to be addressed, designing successful security and privacy approaches can prove to be the first stepping stone in integrating wireless communication techniques with e-health applications. Approaches such as trust negotiations can help build the trust of customers in e-health applications by providing secure access to their Electronic Health Records (EHR). On the other hand, approaches like Information Accountability (IA) can ensure the privacy of the customers. This paper will review data security and privacy approaches that can enable successful integration of wireless communication with e-health applications.

KEYWORDS

E-health, Security, Privacy, Wireless E-health

1 INTRODUCTION

Telemedicine has been prevalent for a considerable period of time. The growing advancements in wireless technologies have caused telemedicine to steadily grow into e-health. According to the World Health Organization (WHO),

"E-health is the transfer of health resources and health care by electronic means. It encompasses three main areas:

- Delivery of health information, for health professionals and health consumers, through the internet and telecommunications.
- Using the power of IT and e-commerce to improve public health services, e.g. through the education and training of health workers.
- The use of e-commerce and e-business practices in health systems management."

It is clear from WHO's requirements that, for e-healthcare to evolve, it must be integrated with the emerging wireless technologies. However, the wireless technologies used in corporate industries cannot be applied directly to healthcare scenarios as it is. While there a number of issues that need to be addressed for widespread use of e-health systems, this paper will only focus on the data security and privacy aspects of e-health applications. The efforts spent in this field are generally application specific, meeting the requirements of a particular e-health application while not necessarily applicable to other applications. Consequently, developing secure e-health applications meeting privacy requirements become a complex proposition. This paper discusses a few methodologies applicable to e-health applications simultaneously pointing out the obstacles that need to be overcome. This paper, after the introduction in Section I, reviews the impact of wireless technologies in Section II and the characteristic requirements of these technologies in Section III. Section IV summarizes three security measures and one privacy measure that can be employed in e-health systems. Section V discusses the lessons learnt from the methodologies discussed in section IV. Section VI and section VII cover the discussion and conclusion respectively.

2 IMPACT OF WIRELESS TECHNOLOGIES ON E-HEALTH

Wireless technology has been developing at an exponential rate for the past few years. More and more applications are now dependent on the fast-growing wireless technologies. This section discusses how the emerging wireless technologies have a significant impact on e-health applications.

2.1 Existing Mobile Technology: From 2G to 3G to 4G and beyond

Development of wireless technology in mobile phones has consistently improved over the past two decades. The significant increase in the data rates, from 2G to 4G, allows the dissemination of critical medical and health information to be achieved faster. Another notable change with respect to e-health systems is the ability of these technologies to relay information in real time. The services offered by wireless technologies have been upgraded from digital voice and SMS in 2G to integrated high quality audio, video, and data in 3G to dynamic information access and wearable devices in 4G. Dynamic information is important for e-health and m-health applications as it allows health staff and patients to view and transmit information in real-time [1].

2.2 Pervasive Communications

Wireless communication is fast becoming pervasive; spreading gradually to affect all aspects of our day-to-day lives. The advanced mobile technologies can be coupled with the existing wireless technologies (WPANs, WLANs, RFID, Bluetooth, etc.) to create an unimpaired platform for launching e-health applications. This pervasive technology allows e-health applications with low data rates but high power and bandwidth requirements to be deployed without portability and mobility issues present in wired interfaces [1].

2.3 Ubiquitous Computing

Ubiquitous computing integrates computing into the environment, thereby making it available anywhere, everywhere, and at any time [2]. In healthcare, this integration can be made possible with the use of wireless sensor networks (WSNs) and Wearable Wireless Body Area Networks (WWBAN) [3]. Ubiquitous computing as stated by Fong et al [3] has four main benefits in an e-health environment:

- It provides mobility and continuity in a medical environment.
- It can also provide patient status reports by placing several monitors in a home environment.
- It allows patients to manage their healthcare processes thus satisfying patients through online viewing.
- It also provides provisions for medical facilities and specialists remotely.

2.4 Context Aware Mobile Services

Context aware mobile services refer to mobile systems that can sense their surroundings and adapt to their physical environment [1]. In healthcare, for instance, if one encounters a sudden medical emergency, a context aware mobile system will direct the individual to the nearest appropriate health center by using his location. This system will also allow the health professionals to access the individual's necessary medical records. By doing so, it avoids redundant examinations and at the same time gives an estimate for the treatment.

"The integration of emerging wireless solutions into healthcare has become a requirement for an accurate and efficient healthcare delivery; however it raises very significant challenges in terms of interoperability, performance, and security" [4].

3 REQUIREMENTS FROM WIRELESS E-HEALTH SYSTEMS

Wireless communication networks face several issues while being integrated into e-health applications. Some notable issues are interoperability and usability, wireless link reliability, electromagnetic interference (EMI), data privacy and security.

It is difficult to use wireless technologies to maintain accurate patient-related medical records as e-health applications use different formats and architecture. Standardization committees like IEEE 1073 and the European Committee for Standardization (CEN) have formed guidelines for applying wireless technologies in a healthcare environment to ensure that devices can work across a global platform depending on available spectrum and local regulation [3]. Health Level Seven (HL7) is another organization dedicated to managing

interoperability standards for healthcare information [5]. A reliable wireless link is another necessary requirement as it ensures availability of accurate patient-data. It also ensures that the patient receives information on precautionary steps, treatment and/or medication. Sources like mobile devices and other wireless handheld devices can cause electromagnetic interference (EMI) with the medical equipment used in hospitals [1]. An ideal device with no EMI is practically impossible; hence it is essential to manufacture devices with minimum interference.

4 METHODOLOGIES FOR SECURITY AND PRIVACY

Health Information Portability and Accountability Act, HIPAA, although formed in 1996, had its security and privacy policies approved in 2005 [6]. Health Information Technology for Economic and Clinical Health Act, HITECH, increased the security requirements proposed in HIPAA act in 2009 [7]. This emphasizes the growing concern in the security and privacy aspects of adopting e-health applications.

Data security and privacy are very important in an e-health environment. It is essential that patient data can only be accessed, managed and altered by authorized users. Corruption, alteration or leaking of patient data can be fatal or can lead to erroneous judgment by the health staff. It is also important for patient data to be secure from malicious attacks or technology failure.

Privacy, on the other hand, is important as a patient might not want certain medical conditions to be available to insurance companies or family members or co-workers. Hence it is essential that patient-data be accessible only to authorized users, i.e. doctors, nurses, medical staff, pharmacist, etc.

This section discusses three different strategies that can be implemented to address security and privacy issues in e-health applications.

4.1 Trust Negotiation Approach

Trust plays an important role in ubiquitous computing implemented in a medical environment as it involves spontaneous interactions between a patient and a healthcare professional in a decentralized network [8]. A trust negotiation approach, suggested by Elkhador et al [8], can be implemented in a remote monitoring system to ensure the privacy of sensitive patient-data and the secure transmission of Electronic Health Records (EHRs). This trust negotiation approach complements the strengths of the Transport Layer Security (TLS). It suggests that the existing protocols can be improved; the strengths of TLS can be combined with trust negotiations, to form a Ubiquitous Health Trust Protocol (UHTP). UHTP combines three levels of authentication with TLS version 1.0 - it authenticates the healthcare professional, the device in use, and the environment of access. These combined together are referred to as the trust negotiation approach.

In this scheme, trust negotiation is multilayered. Three layers of authentication are needed. Elkhodr et al outline the three levels of trust negotiation by showing how a health professional can access a patient's healthcare records. Firstly, the healthcare professional needs to provide a username and password in order to authenticate himself with the healthcare server. Secondly, his mobile device and SIM card must be registered. This is done by using an IMEI number which is unique to every device. Finally, he must be present either within an appropriate predefined range of the patient's home or at an authorized location.

As trust negotiations take place only after the TLS session is established, this approach ensures that the trust negotiations are processed over a secure communication channel. This guarantees the security of the digital credentials exchanged between the client and the server. TLS also ensures that access control decisions are based on attributes rather than identity. These access control decisions are taken in the third layer of trust negotiation.

The third layer of authentication is a two-step process. The first step is Match Location (ML), where the digital credentials; the GPS location of the healthcare professional, are exchanged between the client and the server. If the location of the professional is not either within an appropriate predefined range of the patient's home or at an authorized location, the Match Location function

will deny access to the healthcare professional. If access is granted depending on his location then the third layer of trust negotiation will proceed to step two; check for Role Based Access Control (RBAC). RBAC defines access rights and permissions assigned to a particular healthcare professional to access a particular EHR [8]. The healthcare professional can access the health records only after the server authenticates his access to the records.

4.2 Rolling-Code Cryptographic Approach for a Diabetes Therapy System

A diabetes therapy system is a real time remote monitoring system that works on wireless communication links. It consists of a glucose monitoring system and an insulin delivery system. According to studies done by Li et al [9], passive (eavesdropping of wireless communication link) and active (impersonation and control of medical devices) attacks are both easy to launch on such a system using public domain information and off-the-shelf hardware. Security attacks on a diabetes therapy system can lead to either hyperglycemia or hypoglycemia. Li et al [9] suggest a rolling-code cryptographic approach and Body Coupled Communication (BCC) to counter these security attacks.

Rolling-code algorithms are currently used in remote entry systems for automobiles and buildings [10]. The same concept is applied to an insulin delivery system [9], as they have similar characteristics- one-way communication, low data-rate, and high security requirements. An insulin delivery system consists of a remote control and an insulin pump. Li et al propose a system with an encoder in the remote control and a decoder in the insulin pump.

This insulin delivery system shares an encryption key. This key encrypts a number in the sequence counter of the encoder and increases it by one for every packet. It then transmits the data. The insulin pump decrypts this data using the shared encryption key. The decrypted sequence number in the decoder is then compared with the receiver's sequence counter. Ideally, the code is considered valid only if the numbers match. Since it is very unlikely to get a perfect match, the code is considered valid for a predefined range of numbers. This technique makes it extremely difficult for attackers to hack the device PIN or launch replay attacks as the rolling code changes after every transmission.

4.3 Body-Coupled Communication (BCC) for a Diabetes Therapy System

Body-Coupled Communication (BCC), a human-centric connectivity scheme, proposed by Baldus et al [11] uses the human body as its medium of transmission. It has a limited range of communication due to the close proximity of the human body.

Li et al [9] perform three sets of experiments to show the effectiveness of using a body-coupled communication network over using air channels for a diabetes therapy system. They use a function generator as a transmitter, a middle-wave/short-wave active loop antenna, electrodes, and a Universal Software Radio Peripheral (USRP) as a receiver.

The first set of experiments is set-up to determine the frequency band for BCC. They decide to use the frequency of 5 MHz with maximum spur-free dynamic range (SFDR) of 84 db. SFDR is a measure of signal strength relative to noise level. It is noted that the SFDR of BCC is same as that of the remote control at a distance of 0.5m.

The second set of experiments show BCC's defense against passive eavesdropping attacks. In this case, the function generator transmits a 5 MHz signal via electrodes attached to the human body. USRP mimics an attacker trying to eavesdrop on the communication link. The output power is adjusted to show a comparison of the results between using an air channel and a BCC channel.

Similarly, the third set of experiments show BCC's defense against active attacks. In this case, the function generator mimics an attacker trying to actively control the medical device. The result between using an air channel and a BCC channel is compared again.

A comparison of the results of the experiments performed by Li et al [9] clearly show that the SFDR of the signal is close to 30-40 dB less while

using BCC channels than in the case of using air channels used by the remote control. A low SFDR makes it difficult for attackers to eavesdrop on communication links. It also makes it difficult for them to control the device from a distance.

4.4 Information Accountability

Information security, patient privacy, and health information interoperability are three concerns addressed by Information Accountability (IA) while adopting e-health systems and health information sharing [12]. Gajanayake et al [13] show how privacy can be managed in e-health by handling the access and use of information mutually in an IA environment. This means that while the patient is notified of the access and use of their information, the user of this information must also be warned of the tasks he/she is about to perform and its ramifications.

In an e-health scenario, every time a medical professional uses/accesses information, he/she is accountable for it. However, it must also be noted that medical professionals with common interests can share information amongst them [13].

Gajanayake et al [12] identify the three main components of an Information Accountability framework as WHO- the parties who are held accountable or can be held accountable, WHAT- they are held accountable for, and HOW- they are held accountable

Their article [12] discusses the three components of an IA framework by considering a patient who has his Electronic Health Record (EHR) already stored on the server. In order to receive treatment for a medical condition, he consults his doctor. The doctor in turn needs to access the patient's EHR. Hence the patient must give complete access to his doctor. The patient also gives partial access to his mother as certain medical conditions require family health records for treatment. The doctor then discusses his patient's issues with another medical professional with similar interests. When this medical professional tries to access the patient's information, the IA agent informs the patient about the request. In this case, the patient grants the medical professional complete access as it is for his well-being. At this point in time, the patient's information is being shared securely across multiple networks with multiple entities. The IA agent ensures that the data, at all times, is shared and managed with the patient's consent. The IA agent also notifies the patient every time his information is accessed. In the above case, if the medical professional accesses the patient's information in spite of him refusing access, the IA agent will warn the medical professional of the illegal access/use of the patient's information. The medical professional's actions, in such a case, can be traced back to him/her and he/she would be held accountable for them.

5 LESSONS LEARNT

It is imperative to develop a standard or measure that can be implemented in general to all e-health systems. The trust negotiation approach and information accountability mechanisms discussed above are two methodologies which can be implemented in general to most e-health systems. For instance, the trust negotiation approach, along with the strengths of Transport Layer Security (TLS), can provide a significant improvement in overcoming security concerns compared to traditional identity-based only access control techniques. The advantage of such an approach is that the patient's EHRs can only be accessed by authorized health professionals using registered devices at authorized locations [8]. Information Accountability (IA) is an example of another approach that can be implemented to most e-health systems to address the privacy and confidentiality issues. This approach increases the effectiveness and efficiency of healthcare delivery without enforcing rigid access restriction [13]. Although control over the use of information is imperfect and exceptions are possible, it ensures that violators can be identified and held accountable for their actions. Due to the transparent nature of IA, patients have an increased confidence over the security of their data. Approaches mentioned above, when coupled with the existing security and privacy protocols specified by HIPAA [6] and HITECH [7], can ensure satisfactory e-health systems with respect to the security and privacy aspects.

6 DISCUSSION

Achieving uniformity in health system platforms can prove to be difficult due to the intricate details pertaining to health care and patient-related data. Even in developed countries, interoperability is one of the major concerns shared by most e-health systems. While wireless technologies have been developing at a meteoric rate over the past decade, integrating them with growing health platforms prove to be a major cause of concern. For national implementation of e-health systems, it is imperative that all systems are based on a pre-specified format or platform. This is important because it can prove to be extremely difficult and expensive to have security and privacy measures for varying e-health systems and applications based on the compatibility of the platforms. Gajanayake et al discuss in [13] how health information exchange using information accountability can be very complicated when all health systems do not use the same format and architecture.

7 CONCLUSION

Data security and privacy form an integral part of any wireless network. However, its importance cannot be undermined in an e-health network where a patient's treatment or even his life depends on the reliability of the network. One can put trust in such systems only when it can be guaranteed that the e-health system is secure from all kinds of threats and the integrity of the data is constantly preserved. The methodologies discussed are promising in theory but face concerns in terms of their practical implementation. E-health can progress as a promising future only when sensitive concerns like data security and privacy of patient-related data are addressed. The complete integration of e-health application with secure wireless networks can be a major step towards its success.

8 REFERENCES

[1] El Khaddar, M.A.; Harroud, H.; Boulmalf, M.; ElKoutbi, M.; Habbani, A., "Emerging wireless technologies in e-health trends, challenges, and framework design issues," *Multimedia Computing and Systems (ICMCS), 2012 International Conference on* , pp.440-445, 10-12 May 2012.

[2] Venkataramana, Y., "Pervasive Computing: Implications, Opportunities and Challenges for the Society," *Pervasive Computing and Applications, 2006 1st International Symposium on*, vol., no., pp.5,5, 3-5 Aug. 2006.

[3] Fong, B., Fong, A C. M. and Li, C. K. (2011). Telemedicine technologies: information technologies in medicine and telehealth, John Wiley and Sons, Ltd, ISBN: 9780470745694.

[4] World Health Organization, "Mhealth: new horizons for health through mobile technologies," 2011.

[5] "Health Level Seven International: About HL7", http://www.hl7.org/about/index.cfm [Nov 18, 2013]

[6] "U.S. Department of Health and Human Services: On HIPAA Privacy and Security Rules", http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/hipaarules.html [Nov 20, 2013]

[7] "U.S. Department of Health and Human Services: On HITECH Act", http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html [Nov 20, 2013]

[8] Elkhodr, M.; Shahrestani, S.; Hon Cheung, "Enhancing the security of mobile health monitoring systems through trust negotiations," *Local Computer Networks (LCN), 2011 IEEE 36th Conference on*, vol., no., pp.754,757, 4-7 Oct. 2011.

[9] Chunxiao Li; Raghunathan, A.; Jha, N.K., "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, vol., no., pp.150, 156, 13-15 June 2011.

[10] Alrabady, A.I.; Mahmud, S.M., "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," *Vehicular Technology, IEEE Transactions on*, vol.54, no.1, pp.41,50, Jan. 2005.

[11] Baldus, H.; Corroy, S.; Fazzi, A.; Klabunde, K.; Schenk, T., "Human-centric connectivity enabled by body-coupled communications," *Communications Magazine, IEEE*, vol.47, no.6, pp.172, 178, June 2009.

[12] Gajanayake, R.; Iannella, R.; Sahama, T., "Sharing with Care: An Information Accountability Perspective," *Internet Computing, IEEE*, vol.15, no.4, pp.31, 38, July-Aug. 2011 doi: 10.1109/MIC.2011.51.

[13] Gajanayake, R.; Iannella, R.; Sahama, T., "Privacy by information accountability for e-health systems," *Industrial and Information Systems (ICIIS), 2011 6th IEEE International Conference on*, vol., no., pp.49, 53, 16-19 Aug. 2011.