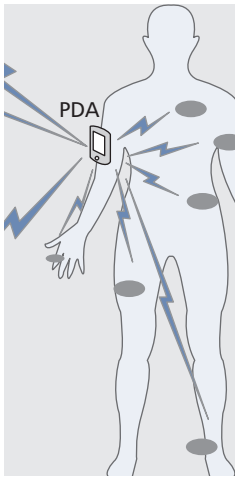
PRIVACY AND EMERGENCY RESPONSE IN E-HEALTHCARE LEVERAGING WIRELESS BODY SENSOR NETWORKS

JINYUAN SUN, UNIVERSITY OF FLORIDA
YUGUANG FANG, UNIVERSITY OF FLORIDA AND XIDIAN UNIVERSITY
XIAOYAN ZHU, XIDIAN UNIVERSITY



The authors provide detailed discussions on the privacy and security issues in e-healthcare systems and the viable techniques for these issues. They also demonstrate the design challenge in the fulfillment of conflicting goals.

ABSTRACT

Electronic healthcare is becoming a vital part of our living environment and exhibits advantages over paper-based legacy systems. Privacy is the foremost concern of patients and the biggest impediment to e-healthcare deployment. In addressing privacy issues, conflicts from the functional requirements must be taken into account. One such requirement is efficient and effective response to medical emergencies. In this article, we provide detailed discussions on the privacy and security issues in e-healthcare systems and viable techniques for these issues. Furthermore, we demonstrate the design challenge in the fulfillment of conflicting goals through an exemplary scenario, where the wireless body sensor network is leveraged, and a sound solution is proposed to overcome the conflict.

INTRODUCTION

Advances in wireless communications and computing technologies have lent great forces to the migration of healthcare systems from paper-based to electronic health record (EHR)-based, giving rise to increased efficiency in human operations, reduced storage costs and medical errors, improved data availability and sharing, and so on.

Electronic healthcare (e-healthcare) offers great convenience to patients and healthcare providers, and improves the quality of life. One such example is the home care application based on wireless body sensor networks (WBSNs), where healthcare professionals remotely monitor patients and provide consultation services. Home care enables patients to retain their living style and causes minimal interruption of their daily activities. In addition, it significantly reduces hospital occupancy rates, allowing more critical patients and patients needing in-hospital treatment to be admitted.

Despite the tremendous benefits, e-healthcare easily incurs threats that are impossible or very rare in paper-based systems. In particular, privacy and security breaches have already penetrated e-healthcare systems, including EHR theft and the selling of EHRs for monetary gain [1]. Thus, there is an urgent need for the development of security architectures/mechanisms that are imperative for safeguarding confidential or sensitive information wherever it digitally resides.

The design of e-healthcare systems is envisioned to be complex, in that highly confidential medical data are the basis for almost all operations. The creation, modification, deletion, storage, access, and sharing of such data need strict regulations. Moreover, the training and education of medical personnel are equally important to ensure compliance with regulations and privacy policies.

Due to the various and stringent requirements of e-healthcare systems, cautions must be taken in the design and development to prevent sacrificing any requirement(s) in the realization of another. Privacy is the foremost issue concerning patients in e-healthcare. Without privacy guarantees, patients' EHRs may be leaked to cause life-changing consequences such as difficulties in obtaining insurance or employment, or being discriminated against for having certain diseases. Most important, e-healthcare systems lacking privacy guarantees cannot be psychologically accepted by the public and hence are not likely to be advocated and implemented. However, in certain special circumstances, such as emergencies, privacy requirements must be overridden by the functional requirement (i.e., saving lives).

In the remaining sections we discuss the privacy and security requirements in e-healthcare systems, elaborate on the techniques to fulfill these requirements, address the challenge of conflicting goals, and propose a solution based on WBSNs to overcome the challenge.

This work was partially supported by the U.S. National Science Foundation under grants CNS-0916391, CNS-0716450 and CNS-0626881. The work of Zhu and Fang was also partially supported by the 111 Project under Grant B08038.

1536-1284/10/$25.00 © 2010 IEEE

WBSNs

As wireless technology and e-healthcare evolve, patients increasingly opt for home care and remote monitoring services offered by healthcare providers. Body sensor networks (BSNs) are indispensable for home monitoring applications, which reduce the hospital occupancy rate. BSNs are also of paramount importance for monitoring patients in the waiting area of the emergency room (ER) [2], where the deterioration of health conditions is detected, and life-endangered patients are admitted correspondingly. The network architecture of home monitoring is illustrated in Fig. 1. Body sensors serving different monitoring purposes (e.g., pulse oximetry sensor, ECG sensor, blood pressure sensor, motion sensor) are attached to or embedded into the human body. In order to provide freeness and flexibility for patients' daily activities, WBSNs are desired where the controller (i.e., the PDA in Fig. 1) wirelessly delivers monitored data to the monitor center. WBSNs are also necessary when the patient is away, and hence the home PC cannot be relied on. WBSNs feature very short-range communications between the sensor and controller, as well as between sensors (not shown in Fig. 1), using Bluetooth and Zigbee radio technologies. Outside the WBSN, the PDA can communicate with the home PC through Bluetooth connection when the patient is home. The wireless links between the PDA or home PC and the remote servers are in general based on Wi-Fi or WiMAX radio. The home PC can also access the Internet using wired connection.

WBSNs resemble wireless sensor networks (WSNs) in many aspects such as the constrained resources of sensor nodes. On the other hand, WBSNs bear unique features and challenges in terms of sensor selection, sensing technology, networking and security design issues, and so on. For instance, body sensors should be easy, comfortable to wear, and non-obstructive; the reliability of sensor nodes is critical in emergency situations and thus is required to be very high; the communication range is extremely short, rendering most attacks impossible or very difficult. A thorough survey on the challenges and opportunities of BSNs is provided in [3]. In this article we focus on the unique privacy and security issues introduced by incorporating WBSNs as a vital component of the e-healthcare system. Specifically, the incorporation necessitates an additional privacy requirement, location privacy, besides anonymity and unlinkability, described later, for general e-healthcare privacy. It also demands the employment of suitable mechanisms for authentication and encryption *within* WBSNs. It is clear in later sections that WBSNs serve as a building block in addressing emergency response issues in the proposed solution.

Location privacy should be guaranteed in the home care scenario whenever emergency response is not needed. In this scenario the WBSN deployed to monitor a patient can be exploited to track the patient's whereabouts through the IP address of the PDA when it wirelessly transfers data to the server. The most attractive feature of home care is that patients can enjoy ease and comfort of living with minimal changes while being treated. The wireless nature of the WBSN enables the patient to engage in daily activities without much constraint. The aggregator/controller (e.g., PDA, smartphone) collecting data from body sensors may send the monitored data periodically and critical data in real time for health evaluation (either upon detecting abnormal conditions or upon a physician's query). When the patient is in normal health condition (i.e., emergency response is not needed), he/she should be considered a regular user leveraging wireless networks to transfer the monitored data. In this case location privacy of the patient should be preserved as is required for regular network users. To satisfy this requirement, an anonymous communication substrate such as [4] will be needed where the origin (the IP address) of the transmitted data is obfuscated. However, patients' location information is indispensable for emergency response; hence, the location privacy requirement should be overridden.

Authentication and encryption within WBSNs require mechanisms different from those for general e-healthcare systems, due to the very limited resources of body sensors and the complexity of public-key-based operations typically present in e-healthcare systems. Although many 5 attacks become impossible (e.g., physical tampering) or extremely difficult (e.g., interception, modification, injecting bogus messages) due to the attachment/embedment of body sensors and the short communication range, security schemes should be in place as long as possibilities for attacks still exist. Recently, efficient authentication and encryption schemes leveraging the unique functionalities of BSNs have been proposed. These schemes rely on the physiological

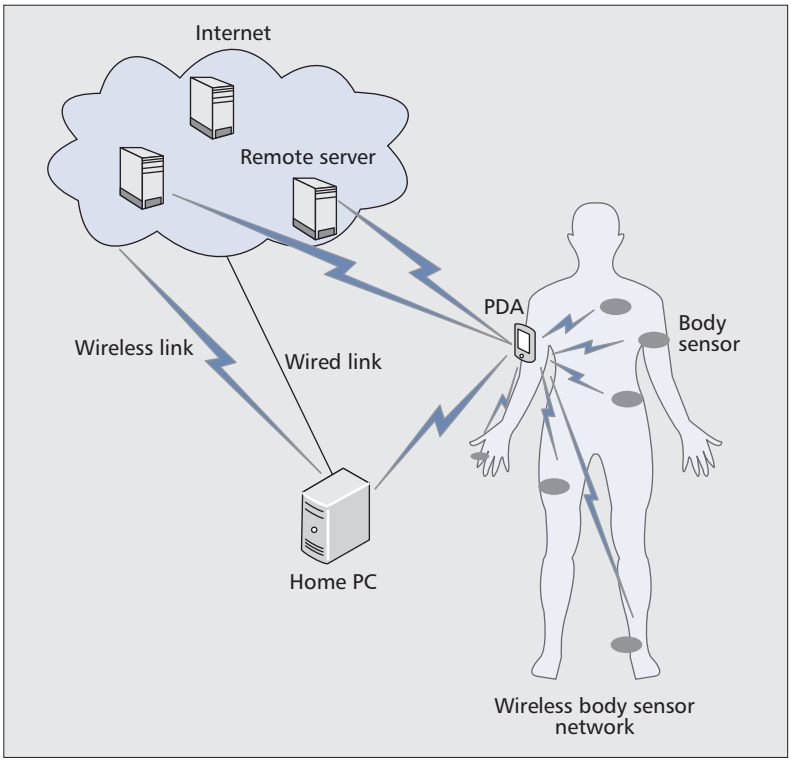


Figure 1. *Home monitoring based on wireless body sensor networks.*

EHR refers to a patient's medical record created, stored, transferred, and accessed digitally, as opposed to the traditional paper-based health record. EHR is the central piece of information in realizing e-healthcare.

values (e.g., inter-pulse interval, heart rate variability) derived from sensor-collected biological signals (e.g., ECG or EKG, PPG), to generate symmetric keys for encryption. The encryption may in turn be needed for authentication, such as the challenge-response authentication proposed in [5]. This line of research explores the uniqueness of an individual's biological signals readily available in BSNs, and points out a promising direction for applying cryptography to solving security problems.

Electronic Health Record

EHR refers to a patient's medical record created, stored, transferred, and accessed digitally, as opposed to the traditional paper-based health record. EHR is the central piece of information in realizing e-healthcare. It may record medical data such as radiology images (CAT, MRI, X-ray), laboratory test results, medication, allergy, disease history, billing information, as well as some processed or aggregated medical data (inter-pulse interval, abnormal condition indicator, etc.) monitored by WBSNs.

EHR systems are used in lieu of paper systems to increase physician efficiency, reduce storage costs and medical errors, and so on. An example of successful implementation of EHR systems in the United States is the Veterans Administration healthcare system, with over 155 hospitals and 800 clinics. It is one of the largest integrated healthcare information systems in the world and has been using a single EHR system for years. Despite all the promising factors, EHR systems are not adopted by the majority of healthcare systems. Statistical results [6, 7] show a very low actual adoption rate of EHR in U.S. medical systems.

Among all the barriers to the implementation of EHR systems, privacy and security concerns are arguably the most predominant. EHRs will inevitably be stored in remote servers (e.g., primary healthcare provider, monitoring center) and exchanged over the Internet for cooperative treatment, emergency response, clinical research, and so on, and thus are subject to theft and security breaches. The Health Insurance Portability and Accountability Act (HIPAA) in the United States was established to regulate EHR related operations. Privacy issues particularly are not addressed adequately at the technical level. Therefore, in addition to governmental regulations, standardization and an overall strategy are needed to ensure that privacy protections are built into computer networks linking insurers, doctors, hospitals, and other healthcare providers [8]. The implementation of the standardization or strategy will undoubtedly rely on technical details rarely studied in the research realm and open numerous research opportunities.

As the need for technical details (i.e., the cryptographic realization of secure EHR systems) becomes more clear and urgent, a few recent works followed this line of research, including cryptographic key management schemes, role-based access control schemes, and anonymous authentication scheme. These works mostly focus on a single problem or aspect of the system, and thus would fail when taking other aspects and objectives into consideration. Technical solutions for ensuring privacy and security while causing no further vulnerabilities in e-healthcare systems are yet to come.

Privacy and Security in E-Healthcare: Requirements and Techniques

We provide a non-exhaustive list of privacy and security issues that concern patients and will serve as requirements/objectives in future e-healthcare system design. We also discuss the suitable cryptographic techniques for solving these issues.

Privacy

Privacy is of paramount importance in e-healthcare, since the illegal disclosure and improper use of EHRs can cause legal disputes and undesirable or damaging consequences in people's lives. For example, an employer may decide not to hire people with psychological disorders, an insurance company may refuse to provide life insurance knowing a patient's disease history, people with certain types of disease may be discriminated against by the healthcare provider, or unusual health conditions of a patient could be revealed to the family disobeying his/her will.

Privacy in the e-healthcare environment comprises anonymity and unlinkability requirements. Anonymity is required when the identifying information in the EHRs must be hidden from certain parties; that is, the EHRs cannot be associated with a particular patient by these parties, including insurance providers, researchers, management staff, and any other related personnel who have no appropriate access privileges. On the other hand, primary healthcare providers (physicians, nurses), delegated healthcare providers, emergency medical technicians (EMTs), cashiers, and others should be able to view such information in order to perform treatment and billing. In addition, the patient's device (e.g., home PC, PDA), which can be used to deduce the patient's identity in WBSNs, should not be identifiable.

Unlinkability indicates that multiple EHRs cannot be linked to the same owner. This requirement is necessary because it prevents the profiling of a patient (e.g., by insurance companies or central servers that store patient data). The insurance companies may attempt to learn more information than is allowed by the patient through exploiting the linkage among EHRs. Monitor centers, either independent or within a hospital, offer storage services to patients under home or critical care and retrieval services to authorized healthcare providers. The storage servers are assumed to be curious but honest, meaning that they will attempt to learn the private EHRs of the patient but will not launch attacks on the stored EHRs (e.g., deletion, modification, bogus injection, irresponsive to retrieval requests). It is apparent that anonymity is a prerequisite for unlinkability, since identifying information renders EHRs linkable.

To fulfill the anonymity requirement, one can employ data anonymization techniques to

remove identifying information and achieve the anonymity of EHRs. The anonymization can be performed by the patient or authorized healthcare providers to allow sharing of the anonymized EHRs. However, data anonymization techniques fail to ensure anonymity when (the IP address of) the device transmitting data in WBSNs can be identified. As a result, the aforementioned anonymous communication substrate for location privacy will be necessary in addition to anonymization. Furthermore, the device will be required to authenticate with the storage servers at the monitor center to prevent users who are unsubscribed to the services from abusing the servers. Since such authentication should be privacy preserving, the public key of the device must be anonymous, which can be realized by adopting pseudonyms or anonymous credentials. At this point, it is clear that the anonymity objective in e-healthcare systems is multifaceted and may require multiple techniques to achieve. Negligence in this area will cause failures in the anonymity guarantee. For unlinkability assurance, anonymization is a viable technique in that the removal of common identifiers in the EHRs results in ambiguity. Encryption can also be leveraged to encrypt EHRs and produce ciphertexts that appear random and hence unlinkable. More discussion on suitable encryption schemes for e-healthcare can be found later.

Access Control

Access control is in charge of who can access patients' EHRs and which part(s) can be accessed, to ensure that only authorized parties can gain access to authorized data. This requirement is in accordance with the HIPAA regulation that patient authorizations will be required to use and disclose EHR information for purposes other than treatment and payment [9]. Basically, the identifying information (or protected health information [PHI]) is necessary for treatment and payment where authorization can be exempted. In all other cases, patients have the right to permit the use and disclosure of their EHRs, indicating that access control should be patient-centric. Access control is an intrinsic issue due to the various types of personnel involved in e-healthcare systems.

Role-based access control is the de facto mechanism to deal with authorizations in e-healthcare, where the roles (e.g., physician, nurse, emergency medical technician [EMT], insurance provider, pharmacist, cashier) and their associated access rights can be defined and specified. It greatly simplifies the control task in that access is determined and granted for each role group but not individually. Translating to cryptographic details, the public key used for authentication and secure communications will be constructed from the descriptive string of a role, as opposed to that of an identity (e.g., in an ID-based public key cryptosystem). Fairly often, patients need to be referred to specialists for examination and treatment. The specialists will therefore have temporary access to the entire or partial EHRs during the course of examination and treatment. Temporary access implies the need for potentially frequent assignment/revocation of the roles, which can be fulfilled by means of delegation. Delegation refers to primary healthcare providers delegating access rights to other healthcare providers and specifying the associated validity period. Most commonly, delegation is role-based where a primary healthcare provider delegates his/her role to another provider, and revokes the role upon termination of the delegation period or task. Depending on the policies and applications, onward delegation may be allowed in which the delegated healthcare provider can further delegate another provider. The depth of the delegation chain will normally be defined by the initial delegator (i.e., the primary healthcare provider). Technically speaking, delegation can be realized through proxy signature/certificate and XML-based approaches.

The role-based approach solves the problem of who has access to the EHRs. However, it alone cannot provide granularity in EHR access (i.e., the portion(s) of the EHRs to which a particular role has access), which requires additional mechanisms such as anonymization and encryption. Anonymization has been mentioned earlier as a privacy preservation technique and may also be leveraged for access control. For example, it is convenient to employ anonymization in data mining performed by related parties, such as researchers and insurance providers who possess access rights only to the non-identifying information of the EHRs. Encryption is another option and is more precise in restricting access. The patient and primary healthcare providers can simply encrypt the EHR portion(s) to be accessed by a role using role-based encryption (i.e., the public key used for encryption describes a role). This manifests another merit of the role-based technique: the encryption can be performed in advance even if the potential recipients are unknown.

Authentication

Authentication is a prerequisite for secure operations since the communicating parties must ascertain the legitimacy and authenticity of each other. Hence, an authentication procedure should be executed as the first step of all communications in secure e-healthcare systems. For instance, authentication takes place as patients transfer data to the monitor center or request test results from their physicians, physicians retrieve EHRs for treatment, the primary physician delegates access rights to other physicians, researchers request EHRs for statistical studies, and so on.

Authentication in the e-healthcare context relies on public key infrastructure (PKI), where a cryptographic public/private key pair is indispensable. Assigning key pairs for authentication in e-healthcare systems is challenging, in that most of the aforementioned communications occur in an interdomain fashion. The domain is defined such that a trusted authority can easily be established to assign key pairs for every entity in this (trust) domain, facilitating intradomain authentication. In general, organizations such as hospitals, clinics, insurance companies, research institutes, monitor centers, and ambulatory treatment centers can be considered individual trust

Authentication is a prerequisite for secure operations since the communicating parties need ascertain the legitimacy and authenticity of each other. Hence, authentication procedure should be executed as the first step of all communications in secure e-healthcare systems.

The major difference between encryption and anonymization lies in the assurance of confidentiality, as the remaining portion of an EHR after anonymization is still viewable. Confidentiality is required when the disclosure of some sensitive information in the EHRs is undesirable, even when such information is not identifying.

domains, where a server may be designated in each trust domain to assign key pairs for the employees in the corresponding organization. Moreover, patients will possess a key pair for each domain (or organization) with which they have a business or research relationship. In interdomain authentication, communications involve two independent domains, the key pairs of which cannot mutually authenticate. As a result, a common certificate authority (CA) needs to be found in certificate-based PKI, or the hierarchical identity-based cryptosystem (HIDC) must be adopted in identity-based PKI, to establish a point of trust for the communicating parties. Nevertheless, the certificate-based PKI is inappropriate in the e-healthcare context since it renders the role-based techniques for access control infeasible. In what follows we demonstrate a possibility of establishing common trust for interdomain authentication leveraging HIDC.

The United States has one of the largest integrated healthcare delivery systems, based on an EHR information system VistA. This healthcare delivery system is administered by the Veterans Health Administration (VHA), the healthcare/medical organization of the U.S. Department of Veterans Affairs (VA). Consequently, the federal VA can act as the common ancestor of all VA healthcare providers (VA hospitals, VA clinics, etc.), forming a hierarchy for enabling interdomain authentication among these providers. Outside the VA system, the Office of the National Coordinator was established within the U.S. Department of Health and Human Services (HHS) striving to build the Nationwide Health Information Network (NHIN), which will connect diverse entities that need to exchange health information. NHIN is intended for state and regional health information exchange, integrated delivery systems, health plans that provide care, personally controlled health records, federal agencies, and other networks as well as the systems they, in turn, connect [10]. Within the NHIN, regional health information organizations (RHIOs) have been established in many states in order to promote the sharing of health information. It provides a platform for interdomain authentication among non-VA healthcare providers, as well as between VA and non-VA providers, possibly by incorporating VA as a participant in the NHIN [10]. Let the NHIN be located at level 0 of the hierarchy. VHA and RHIOs, and their affiliated healthcare providers, are located at levels 1 and 2, respectively, as shown in Fig. 2. Employees of the healthcare provider organization and associated patients reside at level 3. The existence of the hierarchical relationship renders HIDC an ideal candidate for interdomain authentication, in that a point of trust can always be found in the hierarchy by any pair of communicating parties.

Confidentiality and Integrity

Confidentiality and integrity are vital in EHRs. In particular, confidentiality ensures that the (entire or partial) EHR is viewable only to parties with proper authorizations (i.e., decryption keys), and is achieved by encryption primitives. Encryption was mentioned earlier as one of the techniques (another being anonymization) to be used with role-based approaches for fine-grained access control. The major difference between encryption and anonymization lies in the assurance of confidentiality, as the remaining portion of an EHR after anonymization is still viewable. Confidentiality is required when the disclosure of some sensitive information in the EHRs is undesirable, even when such information is not identifying. For example, patients with certain types of disease may feel uncomfortable about releasing related EHR portions for any use other than necessary treatment.

Symmetric or public key encryption can be employed, where the former requires a shared secret key between the encryptor and decryptor, and the latter can utilize the public/private key pairs assigned for authentication. Apparently, public key encryption suits e-healthcare applications since it provides an avenue for role-based techniques. The traditional encryption schemes are most suitable for cases in which the encryptor learns the public key(s) of the decryptor(s) prior to carrying out the encryption. Frequently in e-healthcare applications, the encryption of EHRs will take place without the encryptor's knowledge of the *specific* decryptor(s). For instance, patients' EHRs are stored in ciphertext for future treatment by healthcare providers; the encrypted monitored data from WBSNs are outsourced to storage servers for potential emergency use by EMTs. Furthermore, the retrieval of the encrypted EHRs should be precise and efficient, in that only the most relevant EHRs or EHR portions should be obtained. Considering these features of e-healthcare systems, additional techniques must be incorporated into the traditional public key encryption schemes. To elaborate, the encryption should be role-based which eliminates the knowledge of specific future decryptor(s). In addition, public key encryption with keyword search (PEKS), or simply searchable public key encryption, is a desirable candidate for precise and efficient retrieval. Consequently, role-based PEKS should serve as a building block for confidentiality and access control in secure e-healthcare systems.

Integrity of EHRs must be ensured so that illegal alteration of the original EHRs can be detected by future reviewers. It is critical to satisfy the integrity requirement in e-healthcare systems, since illegal modification of the EHRs (either maliciously or erroneously) may result in life-threatening consequences. Integrity can be achieved by public-key-based digital signature or symmetric-key-based message authentication code. The former is expected to be the dominant technique for e-healthcare applications, and the latter is useful when there is a shared secret key (e.g., between a patient and his/her family or primary physician) for EHR access. Another popular (non-cryptographic) approach to integrity guarantee is the watermarking technique applied in medical information security. This technique ensures both integrity and authenticity of the EHRs (e.g., images, texts, videos, audio) in which the watermark is embedded. The challenge in watermarking is to yield minimal impact on the quality of the original EHRs. As a result, watermarking can be employed for integrity

assurance so long as the distortion is acceptable for the purpose of the application (e.g., diagnosis). Otherwise, the cryptographic approaches mentioned above should be leveraged to avoid medical incidents caused by inaccurate or wrong diagnosis.

Others

Other security requirements, including availability and accountability, must also be satisfied. The most common attack on availability is denial of service (DoS) or distributed DoS (DDoS). The attacker may flood the servers storing EHRs with continuous bogus authentication requests (recall that authentication is required prior to secure communications) to cause irresponsiveness at the server, hindering critical data retrieval. When monitored data are transmitted from WBSNs to the monitor center, the attacker can launch a jamming attack, rendering the wireless channel saturated and unavailable, and thus cause delay in the delivery of critical data. DoS (or DDoS) and jamming attacks remain difficult to thwart. The best solution so far is to alleviate the impact of such attacks by means of signal processing.

Accountability, consisting of traceability and non-repudiation, provides the possibility to trace and identify the party that misbehaves, and subsequently hold this party responsible. The definition of misbehavior is application-specific, and comprises a wide range of activities violating regulatory, policy, or security requirements. Misbehavior may include illegal disclosure of EHRs, abuse of access rights for illegitimate purposes, unauthorized modification of EHRs, and collusion (e.g., between physicians and insurance companies) for monetary gain. To enable accountability and discourage misbehavior, audit trails and digital signatures should be used in combination. Audit trails are available in many systems as the data logger to record transactions and events for statistics, quality of service, or security purposes. In e-healthcare systems audit trails should be in place to trace the sources that break the rules and cause damages. Moreover, digital signatures on transactions and events should be mandatory and also recorded, preventing the signer's repudiation of misbehavior detected in the audit trails.

The Proposed Solution for Privacy and Emergency Response

Generally speaking, the security requirements in e-healthcare systems can easily be fulfilled individually, by either cryptographic techniques or other approaches (e.g., anonymization, watermarking). The complication and challenges arise from taking several, and possibly conflicting requirements into consideration. In this article we identify one such challenge, which is due to the requirements for preserving patient privacy and for efficient response to emergency situations in the home care applications leveraging WBSNs. We explicitly consider the scenario where the home PC or PDA of a patient transmits monitored medical data to a monitor center, facilitating emergency treatment carried out by an emergency medical technician (EMT). In the following descriptions we use monitored data to refer to the EHRs produced by the WBSN in our scenario, in order to distinguish from the general EHRs in e-healthcare systems.

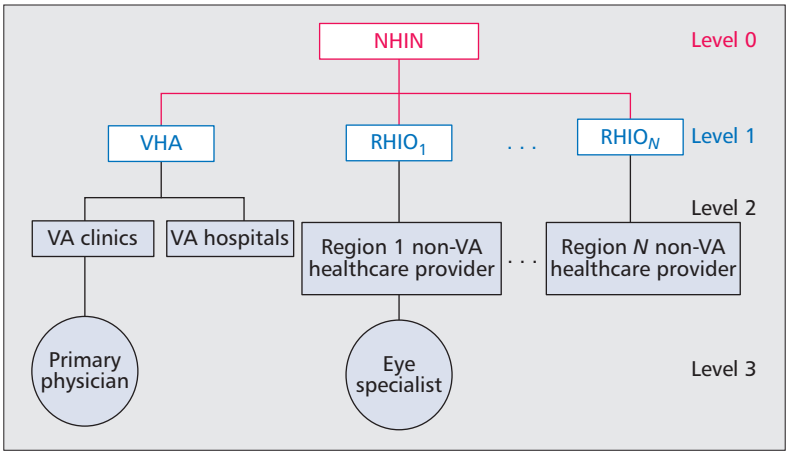


Figure 2. *Logic diagram of e-healthcare hierarchy in the U.S.*

As mentioned previously, the privacy requirements of the patient and his/her EHRs should be overridden in emergency care, where the patient's consent on the use and disclosure of EHRs can be waived. However, such emergency situations should not create a backdoor for attacks and misbehavior. Therefore, patient privacy must still be guaranteed against the EMT whenever it is not needed for emergency care. A potential privacy breach in the emergency scenario is the linkability of monitored data by the EMT. In particular, the role and access rights of the EMT differ from those of the primary healthcare providers, in that the EMT is interested in the most relevant data for efficient and effective emergency response. These data are typically recorded within the past few days (e.g., 3–5 days) and indicate the cause of the emergency. The primary healthcare providers, nonetheless, will demand more data for evaluating the patient's health condition and performing routine medical care. Ensuring unlinkability in emergency responses is a highly challenging task. On one hand, the EMT should be able to obtain the relevant data for successful medical aid. On the other hand, irrelevant data stored in the same server but access to which is not granted to the EMT should not be linked by the EMT to have originated from the same patient. We subsequently propose a solution to address the conflicting goals of unlinkability and emergency response. Note that the anonymity and location privacy requirements are overridden in emergency situations due to the need for effective and timely medical aid by the EMT. However, all privacy requirements (anonymity, unlinkability, and location privacy) should be fulfilled in the patient's interactions with the storage server, which has no right to access the monitored data or any other EHRs.

Our solution is mainly based on anonymous credential, pseudorandom number generator (PRNG), and proof of knowledge. We describe the basic technical procedure as follows:

1) The patient registers at the credential

Timely availability of critical medical data can save people's lives in emergency situations and thus has become an important issue to medical industries. E-healthcare strives to achieve this goal by handling patients' data electronically rendering them ubiquitously available.

authority, located at the monitor center where the patient is serviced. The registration is essentially a procedure in which the patient obtains an anonymous credential from the credential authority for future authentication with the storage server at the monitor center. This procedure is constituted by a commitment phase, a signature phase, and a credential derivation phase. In the commitment phase the patient (i.e., his/her PDA) sends (C, PK) to the authority, where C is a commitment on patient-chosen secrets (α,β) and PK is a proof of knowledge for the correct formation of C. In the signature phase the authority signs C, and returns the signature and other information for forming the credential to the patient. In the derivation phase the patient derives his/her credential using both the information returned by the authority and his/her own secrets. Note that this credential will never be revealed after the derivation. The patient only needs to prove the possession of such a credential in the authentication with the storage server. The anonymous credential guarantees patient anonymity during the data storage in 2), even if the storage server is allowed to collude with the credential authority.

2) The PDA randomly selects a secret seed η to feed into the PRNG, which generates pseudo-random serial numbers ($s_1 \cdots s_n$) at the output, each for an update interval (e.g., every other day) of the monitored data. The number of s_is generated in time period j, denoted l_j, is also recorded by the PDA. The PDA then compute tags based on the serial numbers as $t_i = (\mathrm{H}(s_i))^{\alpha}$ for $i = 1 \cdots n$, such that t_is appear random and unlinkable, where H denotes a cryptographic hash function. The PDA attaches t_i to the monitored data sent in the ith update interval (which falls into a time period, say j) and stores them in the server. The monitored data contain two parts: the outcome of anonymization (i.e., de-identifying information), and the remaining portion encrypted under the EMT's role-based public key using PEKS. After delivery to the storage site, the monitored data, t_is, and s_is are erased from the PDA. All the s_is and t_is can be efficiently regenerated by η, l_js, and α. If the data are to be accessed by other roles (e.g., primary healthcare providers), only the identifying portion of the monitored data need be re-encrypted for each different role. This reduces the extra communication and storage overhead incurred in encrypting the entire data.

3) When the body sensors detect abnormal signals indicating a possible emergency, the PDA immediately contacts the primary physician who will evaluate the situation and request emergency services if necessary. If the primary physician is irresponsive in a predefined (short) time, the PDA will automatically place an emergency call and seek rescue. The EMT at the emergency scene will demand relevant data to assist in the recovery of the patient. Specifically, the EMT sends the date range of the monitored data he/she is interested in to the PDA. The PDA may only accept a reasonable range of recent dates that can contain several time periods. Based on the date range and l_js, the s_is for the desired data can easily be reproduced by inputting η into the PRNG. The serial numbers are in turn leveraged to reconstruct the corresponding t_is, which will be returned to the EMT for retrieving the relevant data from the storage site. Since t_is are unlinkable and only necessary t_is are returned, the EMT cannot arbitrarily review patient data that are irrelevant to emergency care.

The proposed solution achieves the conflicting goals of unlinkability and emergency response. The solution can be considered a stringent access control mechanism the patient exercises on the EMT, enabling the EMT to properly perform medical care while restricting the access to only necessary data. Due to space limitations, the design rationale, detailed descriptions, security and efficiency analysis, and possible enhancements are covered in our technical paper.

Conclusion

Timely availability of critical medical data can save people's lives in emergency situations and thus has become an important issue to the medical community. E-healthcare strives to achieve this goal by handling patients' data electronically, rendering them ubiquitously available. This article addresses patient privacy, one of the most serious concerns of patients and the biggest impediment to e-healthcare deployment. In designing secure e-healthcare systems, we must also consider the conflicts from various functional requirements, one of which is efficient and effective response to medical emergencies. In this article we provide detailed discussions on the privacy and security issues in e-healthcare systems and corresponding viable solutions. We also point out the design challenges in the fulfillment of conflicting goals through an exemplary scenario where wireless body sensor networks are leveraged, and a sound solution is proposed to overcome the conflict. This article is intended to provide a starting point for developing secure and feasible e-healthcare systems.

References

[1] P. Ray and J. Wimalasiri, "The Need for Technical Solutions for Maintaining the Privacy of EHR," *Proc. 28th IEEE EMBC*, Sept. 2006, pp. 4686–89.

[2] D. W. Curtis *et al.*, "SMART: Integrated Wireless System for Monitoring Unattended Patients," *J. Amer. Med. Informatics Ass'n.*, vol. 15, no. 1, Jan. 2008, pp. 44–53.

[3] M. A. Hanson *et al.*, "Body Area Sensor Networks: Challenges and Opportunities," *Computer*, Jan. 2009, pp. 2455–58.

[4] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," *Proc. USENIX Security Symp.*, Aug. 2004, pp. 303–20.

[5] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological Signal based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems," *Proc. 28th IEEE EMBC*, Sept. 2005, pp. 58–65.

[6] C. W. Burt, E. Hing, and D. Woodwell, "Electronic Medical Record use by Office-based Physicians: United States, 2005," Nat'l. Center for Health Statistics, 2005; http://www.cdc.gov/nchs/products/pubs/pubd/hestats/electronic/electronic.htm

[7] Nat'l Center for Health Statistics, "More Physicians using Electrical Medical Records," 2006; http://www.cdc.gov/media/pressrel/a060721.htm?s_cid=mediarel_a060721

[8] R. Pear, "Warnings over Privacy of U.S. Health Network," *The New York Times*, Feb. 2007.

[9] G. M. Stevens, "A Brief Summary of the Medical Privacy Rule," CRS Rep. for Congress, 2003.

[10] U.S. Dept. HHS, "Health Information Technology"; http://healthit.hhs.gov/

BIOGRAPHIES

JINYUAN SUN [S] (stellas@ufl.edu) received her M.A.Sc. degree in computer networks from Ryerson University, Canada, in 2005. She received her B.S. degree in computer information systems from Beijing Information Technology Institute, China, in 2003. She was a network test developer at RuggedCom Inc., Ontario, Canada, 2005–2006. She is currently working toward her Ph.D. degree at the University of Florida. Her research interests are in the security protocol and architecture design of wireless networks.

XIAOYAN ZHU (xyzhu@mail.xidian.edu.cn) received her B.E. degree in information engineering in July 2000 and her M.E. degree in information and communications engineering in March 2004, both from Xidian University, Xian, China. She is now working toward her Ph.D. degree at Xidian University and is currently a research visiting scholar at Wireless Networks Laboratory (WINET) in the Department of Electrical and Computer Engineering of the University of Florida. Her research interests include wireless networks, network security, and network coding.

YUGUANG FANG [F'08] (fang@ece.ufl.edu) received a Ph.D. degree in systems engineering from Case Western Reserve University in January 1994 and a Ph.D. degree in electrical engineering from Boston University in May 1997. He was an assistant professor in the Department of Electrical and Computer Engineering of the New Jersey Institute of Technology from July 1998 to May 2000. He then joined the Department of Electrical and Computer Engineering of the University of Florida in May 2000 as an assistant professor, and got an early promotion to associate professor with tenure in August 2003 and to full professor in August 2005. He has held or holds a University of Florida Research Foundation (UFRF) Professorship from 2006 to 2009, a Changjiang Scholar Chair Professorship with Xidian University, Xi'an, China, from 2008 to 2011, and a Guest Chair Professorship with Tsinghua University, China, from 2009 to 2012. He has published over 250 papers in refereed professional journals and conferences. He received the National Science Foundation Faculty Early Career Award in 2001 and the Office of Naval Research Young Investigator Award in 2002, and was the recipient of the Best Paper Award at the IEEE International Conference on Network Protocols (ICNP) in 2006 and the IEEE TCGN Best Paper Award in the IEEE High-Speed Networks Symposium, IEEE GLOBECOM in 2002. He is also active in professional activities. He is a member of ACM. He is currently serving as Editor-in-Chief for *IEEE Wireless Communications* and serves/has served on several editorial boards of technical journals, including *IEEE Transactions on Communications*, *IEEE Transactions on Wireless Communications*, *IEEE Wireless Communications*, and *ACM Wireless Networks*. He was an editor for *IEEE Transactions on Mobile Computing* and currently serves on its Steering Committee. He has actively participated in professional conference organizations such as serving as the Steering Committee Co-Chair for QShine from 2004 to 2008, Technical Program Vice-Chair for IEEE INFOCOM 2005, Technical Program Symposium Co-Chair for IEEE GLOBECOM 2004, and a member of the Technical Program Committee for IEEE INFOCOM (1998, 2000, 2003–2010) and ACM MobiHoc (2008–2009).