Part IV

Security in Pervasive Computing

15

Security Solutions for Pervasive Healthcare

Krishna Venkatasubramanian and Sandeep K.S. Gupta

CONTENTS

Abstract Pervasive healthcare systems use pervasive computing technologies, e.g., wearable medical sensors with wireless interconnects, to increase the modalities and spatiotemporal dimensions in which healthcare services can be provided for improving patient outcomes. Security is very important in pervasive healthcare systems to protect sensitive health information that it collects and manages; therefore, they have to maintain data confidentiality, integrity of data, and provide strong authentication features, thereby controlling unauthorized access of personal health information. This chapter presents an overview of security solutions for pervasive healthcare systems, focusing primarily on three aspects: 1) securing data collected by medical sensors, 2) controlling access to health information managed by the pervasive healthcare system, and 3) legislative framework available for securing healthcare systems.

15.1 Introduction

The goal of pervasive healthcare (PH) is to use pervasive computing technologies to provide round-the-clock healthcare outside the confines of traditional medical establishments, such as hospitals and medical clinics, but rather in

their homes and outdoors. Traditional model for health management consists of *observing symptoms, visiting a doctor, getting treatment*. Pervasive healthcare aims to change this model into one that provides healthcare facilities to individuals anywhere and at any time. It uses large-scale deployment of sensing and communication (wired and wireless) technologies to monitor patients continuously. This allows it to deliver accurate health information to the medical professionals, thereby stimulating timely diagnosis and treatment for health problems.

Pervasive healthcare, therefore, by facilitating improved patient-caregiver interaction, has the potential to provide accurate, timely, and error-free care to all. This is particularly useful nowadays since the population is aging rapidly; medical institutions are facing shortages of medical staff; cost of healthcare is skyrocketing; and incidences of medical errors are at all-time high [11].

Significant advances in communication and sensing technologies has led to the development of intelligent handheld and wearable devices (such as PDAs, cell phones, smart watches, clothes, and bands) that have made it possible to implement a wide range of solutions for PH systems. The health management capability of pervasive healthcare systems makes them ideal for many diverse applications including [1] the following.

- **Mobile telemedicine**: Provides the ability to monitor, diagnose, and treat patients from a distance. This reduces the chances of medical errors and enables timely treatment of patients by providing accurate, real-time, and complete health information to the medical professional. Example usage scenarios include monitoring patients in remote rural locations and reacting immediately in response to a medical emergency (dispatching an ambulance), and providing patient monitoring and treatment for post operative care.
- **Disaster response**: Provides the ability to respond effectively to disasters, where the numbers of patients far exceeds the number that can be handled by the available medical staffs. Using an appropriate pervasive healthcare system, patients can be automatically monitored and doctors' attention can be brought to only those patients who are critical, thereby improving the effectiveness of the response.
- **Pervasive access to patient health data**: Pervasive healthcare systems are designed to collect data from patients over long periods of time. These data are stored in an organized manner so that they can be studied by the patients' caregivers to provide better care. Such large data sets can be useful for studying issues such as response to medicine, demographics of people with specific ailments, possible improvements in the care, improvement in medicine, alternative treatments and diagnosis.
- **Lifestyle management**: Pervasive healthcare systems have the ability to provide personalized care. For example, it can be used by people to improve their health by developing specialized meal and exercise plans.

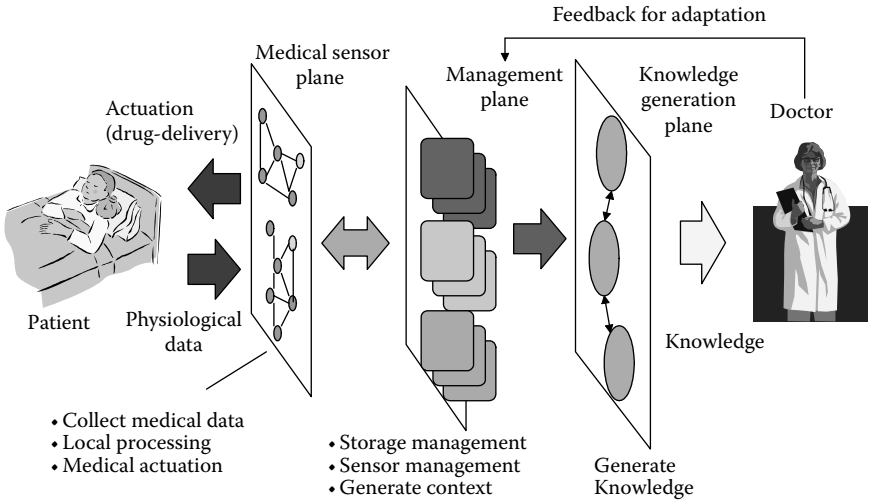

FIGURE 15.1
A generic pervasive healthcare system model.

Figure 15.1 presents a generic model for a pervasive healthcare system. Conceptually, the model consists of three main planes: the **medical sensor plane**, the **management plane**, and the **knowledge generation plane**. The sensor plane provides the capability to incorporate a large number of various types of medical sensors in a pervasive healthcare system. These sensors may have the capability to continuously or intermittently monitor various physiological parameters, such as EKG (electrocardiogram), blood pressure, body temperature, galvanic skin resistance, and motion detection of various body limbs. The sensors may be placed on the patient[1] (wearable) or inside the patient's body. In some cases, these sensors may also have actuation capabilities and can perform tasks, such as drug delivery, under the control of the management plane.

The management plane provides an infrastructure for managing the health data collected by the sensors. It takes raw health data from the sensors, and organizes them into a structured format by generating an Electronic Patient Record (EPR). An EPR collects health data concerning a single patient in a manner that is easy to store and access. It also stores useful information about the patient to assist in better understanding of the data. Further, the management plane provides intelligent indexing and mining capabilities for fast retrieval of pertinent health data and information from EPRs. In addition, the management plane provides functionalities to direct the sensor plane to collect specific stimuli based on the current requirements or actuate specific

[1] The term patient is used interchangeably with the term individuals, to denote any individual who is wearing medical sensors on his body for health monitoring.

treatment. Computational devices such as PDAs, cell phones, PCs, and servers are employed in the implementation of the management plane.

The knowledge generation plane is used for reasoning on the data collected and stored (in EPRs) by the previous two planes. It provides features, such as detection of the occurrence of a medical emergency, the failure of a specific treatment procedure, inconsistencies between the proposed diagnosis and the symptoms. This capability gives the caregivers feedback pertaining to their diagnoses and treatment, allowing them to make appropriate adjustments through the management plane.

15.2 Security Threats in Pervasive Healthcare Systems

A pervasive healthcare system collects and manages health data in an electronic format—EPRs—as compared to the largely paper-based records of today. The usage of EPRs, however, imposes many security risks to the health data that did not exist before with paper-based records. This may lead to unauthorized access and tampering of sensitive health data of patients. The reasons for this new-found vulnerability are:

1. Paper-based health data storage is highly centralized and any copying of this information is tedious and a time-consuming process. With EPRs kept on networked systems for availability reasons, it is accessible from anywhere and is very easy to copy.
2. More and more sensitive information is being included in a patient's EPR for faster and easier retrieval. Examples include HIV status, psychiatric records, and genetic information.
3. The networked nature of pervasive healthcare systems allows the EPRs to be moved across administrative or even national boundaries with ease, thereby circumventing any local legal issues [2].

Therefore the ability of pervasive healthcare systems to continuously collect, exchange, store, and reason, based on electronic health data poses many avenues of abuse of privacy and security. Some of the more probable threats to the pervasive healthcare systems include:

1. Unauthorized access to health data.
2. Deliberate alteration of health data of specific patients, leading to incorrect diagnosis and treatment.
3. Deliberate generation of false alarms or suppression of real alarms raised by the system in case of emergencies.
4. Economic and social discrimination of patients (insurance companies offering health insurance with high premiums to people who have certain chronic problems).

Recently there has been a significant increase in concern, in the popular press and masses, over privacy issues, relating to the electronic health data. Therefore, the viability and long-term success of the technology depends upon addressing the aforementioned threats [2]. Security and privacy preservation in pervasive healthcare has not been investigated in much depth before, and thus provides ample avenues for research. Section 15.3 presents the security solutions for a PH system focusing on preserving the security of health data collected and maintained by the system.

15.3 Security Solutions for Pervasive Healthcare

Security is essential for any system. In the context of pervasive healthcare systems, it is even more important because these systems deal with health information maintained within the EPRs. *The principal idea behind securing pervasive healthcare systems is to preserve patient privacy*. To ensure this, care needs to be taken to prevent all unauthorized access to EPRs in the system.

The notion of providing security in the domain of pervasive healthcare is not different from traditional systems and relies on the maintenance of three basic properties. **Data Integrity**: All information provided is accurate, complete, and has not been altered (during transit and storage) in any way. **Data Confidentiality**: Information is only disclosed to those who are authorized to see it. **Authentication**: To ensure correctness of claimed identity of communicating entities. Here, we present security solutions of pervasive healthcare systems that focus on protecting health data from three different aspects:

- **Securing Medical-Sensor Communication**: Individual medical sensors, used in a pervasive healthcare system, have very small form factors and therefore have limited capabilities. Hence, in general, a complex, computation-intensive security mechanisms (such as Public Key Infrastructure (PKI)) is not suitable for securing medical-sensor communication in the context of pervasive healthcare.
- **Controlling Access to EPRs**: An important property of a medical system is that patients have a high level of control over deciding who accesses their health information. Pervasive healthcare systems use EPRs to store pertinent health information about patients. As many organizations, such as pharmacies, insurance agencies, drug companies, and caregivers, need to gain access to patient EPRs for their own economic needs and to provide better service (e.g., improved drugs and competitive insurance rates), patients should be able to easily control access to their EPRs so that personally identifiable sensitive health information is not released.

- **Legislative Solutions**: Realizing the importance of a legal framework for maintaining for protecting sensitive medical information stored as EPRs, the U.S. Congress proposed a Health Information Portability and Accountability Act (HIPAA) in 1996. All technical solutions are required to address the recommendation proposed by HIPAA and a basic understanding of its provisions is required.

Further, there are two additional issues associated with pervasive healthcare systems; security of wireless communication and physical security of handheld devices. Pervasive healthcare systems make extensive use of wireless communication technologies such as WLAN and cellular phones to communicate health data collected by medical-sensor networks [7]. However both these communication technologies have many security vulnerabilities. The security problems primarily relate to poor encryption algorithms (Wired Equivalent Protocol (WEP))[8, 9, 10] and session management (GSM) [24]. However, the next generation of both technologies have addressed the issues (with 802.11i and 3G systems, respectively)[11, 24].

To provide pervasive health monitoring, the PH systems make use of portable handheld devices that are used by both patients and caregivers. Such devices may store sensitive health information about the patient and cause a serious privacy breach, if stolen or misplaced. Therefore, physical security of the devices involved also has to be considered. Some solutions for this problem include user-device authentication (using biometric [4, 12, 13], RFID [14], and e-tokens [27]), and use of smart cards [15, 17, 16]. However, these issues are outside the scope of our presentation, and are mentioned here solely for completeness reasons.

15.3.1 Sensor Networks Security in Healthcare

In this section we present issues relating to securing communication between medical sensors used in a pervasive healthcare system. In recent years several promising clinical prototypes for implantable and wearable health-monitoring sensors have started to emerge [7]. These devices are being used for continuous monitoring of patients over long periods of time. Much of the work so far has gone into their design to make them stable, biocompatible, power-efficient, and reliable. However, as these sensors are used for collecting health data from patients, ensuring that they do so in a secure manner is equally important.

Security for generic sensor networks has been a prime topic of research over the last couple of years and large numbers of interesting results have been obtained. However, security issues for medical sensors are largely an unexplored area. We need a slightly different outlook while addressing security issues for medical sensors primarily because of the environment (i.e.,

the human body) in which they are placed. One of the most important requirements of medical sensors is that they should not hinder the day-to-day activities of the person who is wearing them. This requires the sensors to be extremely small in size and weight. The computation and communication capabilities of the medical sensors are therefore more constrained than generic sensors. As security adds overhead to the system, care needs to be taken to ensure that this overhead is minimized in case of medical sensors.

One of the first works to address the issue of security for implantable and wearable medical sensors is [3]. It advocates the use of the human body itself as a means of generating cryptographic keys (for symmetric cryptography, as Public Key Infrastructure may be too expensive) for securing intersensor communication. As the human body is an extremely dynamic environment, it can produce many specific physiological values that are time-variant and not easy to guess (are random and from a large range of values). Using these for cryptographic purposes provides strong security and eliminates key distribution. Both the sender and receiver can now measure the physiological values from their environment and use them for security purposes, when they want to communicate [3].

The principal idea behind this scheme is for the senders and receivers to measure a previously agreed-upon physiological values (PV) simultaneously. The synchrony in measurement is required because the values of the PVs are time variant. Once the values are measured, say, the values are K_s and K_r for the sender and receiver, respectively,[2] to send a confidential message, the sender first generates a random session key $K_{session}$, encrypts the payload with it [$C = E_{K_{session}}(Data)$], and then hides the $K_{session}$ using K_s by computing a one-time pad on it ($\gamma = K_{session} \oplus K_s$). It also computes a Message Authentication Code (MAC) on the encrypted message C using the $K_{session}$ ($mac = MAC(K_{session}|C)$) to allow verification and to maintain message integrity. The sender then transmits the message [C, γ, mac] to the receiver, which then uses K_r to obtain $K'_{session}$ from γ ($K'_{session} = \gamma \oplus K_r$). Due to the dynamic nature of the human body, the values of K_s and K_r may not be the same, resulting in the derived $K'_{session} \neq K_{session}$.

In [3], the authors contend that values of PVs measured from the same individual are very close, and any discrepancies in their values are treated as analogous to communication errors [6]. Error correction code (such as majority encoding) is then used to correct the difference. Therefore the receiver performs error correction on $K'_{session}$, yielding $K''_{session}$ ($K''_{session} = f(K'_{session})$, where f is the error correction code). The receiver now computes its own version of the MAC using $K''_{session}$, $mac' = MAC(K''_{session}|C)$. If the values of mac and mac' are identical, then the receiver decrypts C to obtain $Data$, otherwise,

[2] The values being measured, may not be same at both ends because the values are not analog in nature and some discrepancy may arise.

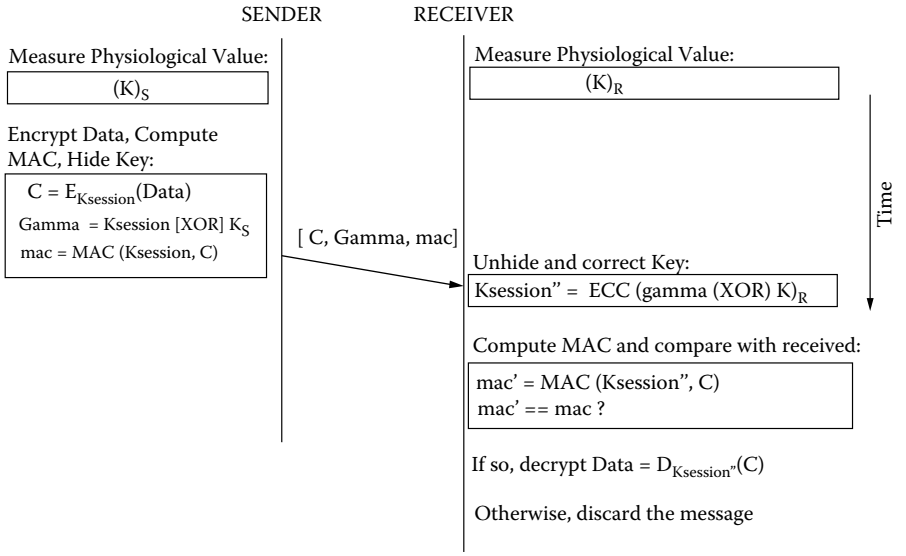

FIGURE 15.2
Secure communication, in body sensor networks, using physiological values.

it discards the message received (Figure 15.2). The pseudocode for this process is given below:

DATA_PROCESS()
1. measure chosen PVs at both sender (K_s) and receiver (K_r) simultaneously
2. if (DataToSend)
3. $C \leftarrow E_{K_{session}}$(Data)
4. $\gamma \leftarrow K_{session} \oplus K_s$
5. $mac = MAC(K_{session}|C)$
6. send(C $\|$ γ $\|$ *mac*)
7. end if
8. if (DataToReceive)
9. $K''_{session} \leftarrow f(K_r \oplus \gamma)$
10. $mac' = MAC(K''_{session}, C)$
11. if ($mac == mac'$)
12. Data = $D_{K''_{session}}(C)$
13. else
14. reject data received
15. end if
16.end if

The choice of PVs is an important issue here. Not all PVs possess the time variance and randomness that is required to effectively hide $K_{session}$. For example, if we choose, blood glucose whose value in humans normally ranges between 64–140 mg/dl [28], as PV, irrespective of its time variance, the range of values is so small that it is vulnerable to brute-force attacks. For similar reasons, the use of PVs like blood pressure and heart rate directly is also not advised. In [4] and [5], the use of more complex PVs such as Inter-Pulse-Interval

(IPI) and Heart-Rate Variation (HRV) have been proposed as suitable PVs for securing implanted biomedical sensor communication, respectively. In both cases the PVs, i.e., HRV and IPI signals, were encoded to 128-bit values. Values of any two measurements of these PVs were found to vary considerably, when measured from two different individuals and were very similar when measured from the same individual. Further, the values varied with time and were not predictable. Similarly EKG (electrocardiogram), which has been shown to uniquely identify individuals [29], can also be used here. More work, however, needs to be done to identify other PVs for this purpose. The use of PVs as security primitives for intersensor communication in pervasive healthcare ensures the confidentiality of the data (through encryption), integrity (through MAC), and effectively authenticates the communicating sensors because of the uniqueness of the PVs[3] with respect to the individuals in whom they are measured.

15.3.2 Controlling Access to EPRs

Preserving the privacy of the information collected and maintained as EPRs by a networked and distributed architecture, like that of PH, is very important. This is especially true, when such information may be accessed by entities other than the patient's caregiver and family, such as pharmacies, insurance companies, and drug manufacturers, for their economic and service needs. Since sharing of patients' health information requires their informed consent, pervasive healthcare systems need access control schemes to capture and enforce the specific needs of each patient. In this section we address the issue of authorization in accessing EPR of patients within a pervasive healthcare system using access control mechanisms.

Preliminaries

One of the frequently used techniques for access control in healthcare systems is Role-Based Access Control (RBAC) [18, 19, 20]. RBAC, first proposed in [22] and [23], is a mechanism for access control that organizes users [in the system] into specific groups called *Roles*. Roles are groups of users formed based on the functions they perform within the system. For example, all users who are doctors within a hospital will be assigned the role of *doctor* and all the nurses in the hospital system will have the role *nurses* assigned to them. RBAC further assigns access privileges to these roles, instead of to each individual user. This decoupling of users' identity from the privileges associated with them provides a greater level of scalability, as opposed to Access Control List (ACL)-based access control schemes that maintain lists of privileges for different users with respect to the resources within the system. The primary advantage, therefore, of an RBAC-based system is its ability to reduce complexity and

[3] In [5], it has been shown that the values of HRV measured from two different individuals vary by as much as 80 bits of Hamming distance. However, two measurements of HRV from the same individual vary slightly (3–8 bits of Hamming distance).

the effort for managing access to large-scale systems. RBAC further defines role hierarchies in order to allow management of relationships between roles within the organization. For example the role of a doctor in a hospital could be a parent role for the role of cardiologist, as a cardiologist is a form of doctor. All privileges associated with the role doctor are inherited by the role cardiologist as well.

Extension of RBAC for Controlling Access to Medical Information

As mentioned before, for healthcare information, the patients themselves must be able to define who can and cannot access their EPRs. In [25] it is argued that access control schemes used in healthcare environments should support two types off policy expression: *general consent qualified by explicit denial (GC-ED)*, and *general denial qualified by explicit consent (GD-EC)*. Example of the former could be a rule, such as all physicians except Dr. X, and of the latter could be no physician except Dr. X. GD-EC is required in scenarios where access needs to be tightly restricted, where it is more convenient to block all users except a few who are explicitly provided access. GC-ED on the other hand is useful for efficiency purposes, for example, using the GC-ED mechanism, a hospital could specify a default set of policies specifying who are prevented by accessing a patient's health information, and the patients can then modify this according to their needs.

In RBAC, as roles can execute only those privileges that are assigned to them and no other, by nature it can easily express GD-EC scenarios. Implementing GC-ED in RBAC is tedious because we would need to define a role explicitly listing all users who need to be given access. If access is to be prohibited for only a handful of users, this role will be very tedious to populate. Using constraints with RBAC has been defined, as a means of denying exercising of privileges for a role that would otherwise be allowed. However, constraints do not provide an elegant solution especially with the role hierarchies of RBAC [18]. For example if a constraint is applied to the role of a clinician, then its child role (doctor) will also inherit the constraints of the role. Therefore we will not be able to easily execute a policy of the form *provide access to all clinicians except Dr. X*.

In [18], the authors have proposed a solution to this problem by presenting a simple extension of RBAC. In their healthcare access control model, a patient's access policy are recorded and enforced through a consumer centric role called *care-team role* (CTR). A CTR consists of four main components: list of roles who are allowed access to the patient's health information, list of roles who are denied access to the patient's health information, the access privileges, and administrative information about the CTR such as its ID and description. Figure 15.3 shows the CTR structure, where all doctors and nurses (except Nurse Y) were allowed read access to the patient's EKG and radiology reports. Similarly, all radiologists are also prevented from reading the patient's EKG and radiology reports. It further needs to be noted that, all roles for which access is denied, override all roles that are equal or more general. Therefore, if all doctors are prohibited from access, then all clinicians

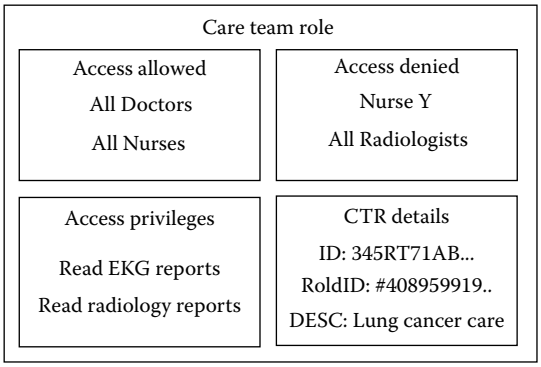

FIGURE 15.3
Care team role structure [18].

would be prohibited, too, unless they are explicitly mentioned in the list of roles who are allowed access. The presence of two lists ensures the implementation of both GD-EC (through the access-allowed list), and GC-ED (through the access-denied list). Figure 15.4 shows the relationship between roles and permissions when using CTR given in Figure 15.3 [18]. Here all nurses are assigned privileges to read both EKG and radiology reports, while a particular nurse Y is denied permission.

Context Awareness in Controlling Access to Medical Information

The aforementioned model modified the RBAC model to support scenarios requiring GC-ED, apart from GD-EC, to facilitate easy expression of patients' wishes regarding access to their EPRs. In [20] the RBAC model is extended in a different way, by introducing the element of context in access control

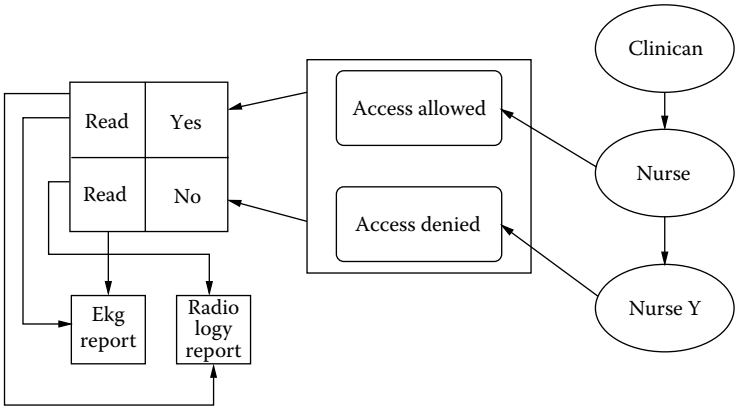

FIGURE 15.4
CTR usage [18].

decisions. The authors argue that access privileges to information in the EPRs for different roles are not static and may vary with the system context. For example if Doctor X had the privilege to access a patient's record now, he may not have one the next day because of his reassignment to another patient (change of context). The ability to describe contexts is an important feature of their work, which is done in the form of a regular expression. Its schema is generic enough to allow the expression of complex context information [20]:

$Context = Clause_1 \cup Clause_2 \cup \ldots . \cup Clause_i \ldots$
$Clause = Condition_1 \cap Condition_2 \cap \ldots . \cup Condition_i \ldots$
$Condition = Context\ Type < OP > Value$

Here Context Type defines a specific property of the system, such as the time and the location; OP is the operator, such as $\leq, \geq, \neq$. Given this means of expressing contextual information, the system provides access to users (e.g., caregivers, pharmacists) based on *authorization policies* (AP), which is defined as a triple $< R, P, C >$ where R is a role, P is the requested permission, and C is the given context (described using the schema given above). When users want to obtain access, they present a *data access request* (DAR) of the form $< U, P', CR >$ where U is the user ID, P is the permission required, and CR is the actual values of the context types. Access is provided to the user if and only if the actual values presented with the context types (CR) of the DAR evaluates as $true$ in the context description (C), $P = P'$ and $U \in R$.

Controlling Access for Managing Medical Emergencies

The Context-Aware Role-Based Access Control (CA-RBAC) was designed for taking context information into consideration when providing access to patients' EPRs. The access provided to the health information is, however, reactive in nature, that is, access is provided only on explicit request from the users. Though adaptive in nature, it only takes into account the current context of the users, compares it with existing rules about privileges to be assigned in such contexts before providing appropriate access. However, what it does not consider is the occurrence of critical events in the system and providing access for this change. An example of a critical event includes a heart attack for a patient whose assigned doctor is not available. The resulting effects on the system due to the occurrence of the critical event is called *Criticality*. Timely mitigation of criticalities is essential for the proper working of the system and access control systems can assist in this process. In the previous example, a smart access control mechanism should therefore be able to find other qualified doctors in the hospital and provide them appropriate access to the patient's EPR. This mitigates the effects of the critical event (heart attack).

Here, if a CA-RBAC model were used, it would not have provided access to the patient's EPRs to any doctor other than the one assigned to the patient

without explicit consent of any kind. In [19], the authors have proposed a novel access control model for handling access control in such emergencies called Criticality Aware Access Control (CAAC). CAAC is designed to provide *proactive* access to handle system emergencies. By proactive we means facilitating continuous monitoring of the system for critical events and in event of observing one, automatically providing an alternate set of access privileges to selected users without any prompting or request.

As the access in CAAC is provided automatically, care has to be taken that it is not provided for longer than absolutely required, for minimizing misuse. Therefore any access provided to users in response to an emergency is temporary and is rescinded after a specific amount of time. The value of this time duration is limited by the window of opportunity (W_o) of the emergency.[4] Every emergency has a duration, called the window-of opportunity, associated with it. This is the maximum time before which mitigative measures have to be initiated and completed for controlling the emergency. If the emergency is not handled within W_o then irreparable damage could ensue, for example, in the event of a heart attack, the window of opportunity for controlling it is 1 hour (in most cases); if not controlled by this time, it may not be possible to save the patient's life. In normal circumstances the CAAC model degenerates to Context Aware RBAC similar to [20]; however, in case of emergencies, the system suspends the Context Aware RBAC model and implements the CAAC model. Figure 15.5 shows the execution model of CAAC [19]. When the system observes a critical event, it moves into a CAAP (Criticality Aware Access Policies) mode where the system implements an alternate set of access policies to facilitate effective mitigation.

15.3.3 Legislative Solutions

Apart from technical solutions proposed, an equally important means of ensuring security of information collected in a pervasive healthcare system is legislative. With a growing rise in the digitization and electronic exchange of medical records, the Health Insurance Portability and Accountability Act (HIPAA) was passed in the U.S. Congress in August 21, 1996, to address information portability and security issues that emerge from this trend. The scope of of HIPAA is threefold: 1) To simplify the administrative overhead in collecting, managing, and accessing EPRs; 2) To prevent healthcare fraud and abuse; 3) Tax-related group plans and revenue offset provisions [21]. Though the scope of HIPAA is considerably larger, we will focus on the HIPAA privacy and security rules that are designed for the prevention of fraud and abuse of medical data. Before proceeding further we need to define the notion of *covered*

[4] The actual duration is defined as the earliest time when either one of the following is true: the criticality has been successfully mitigated, the window of opportunity has expired, or all the mitigative actions that could possibly be taken have been executed and nothing more can be done irrespective of the presence or absence of criticality.

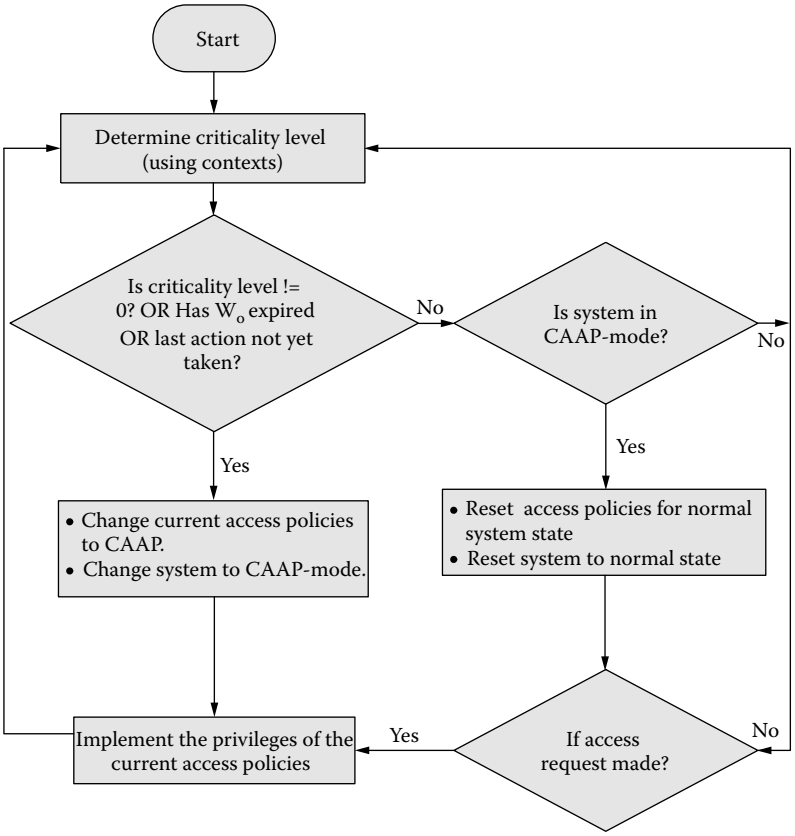

FIGURE 15.5
Execution model for CAAC [19].

entities (CE). A CE includes all entities that deal with collection, storage, and management of health information, health plan providers, healthcare clearing houses, and healthcare providers. All HIPAA regulations apply to CEs only.

The HIPAA privacy rule concerns with defining policies for information flow, rights of patients to access, review, and change their medical data. It defines the notion of personally identifiable health information (PHI) (which can be contained in either electronic, paper, or oral form) and requires that it be protected. It further proposes methods for releasing such information by: 1) removing all identification information from it such as name, geographic locations, telephone numbers, medical record numbers, and health plan IDs; 2) releasing a limited dataset for research purposes, public health and healthcare operations. It further provides certain rights to the individuals concerning their health information, such as 1) the right to provide notice of

any information that a CE released; 2) the right to request restriction on the use and disclosure of health information; 3) the right to access and amend one's medical records; 4) the right to audit disclosure of medical data [21]. However, covered entities have the power to apply discretion on honoring any of these rights of individuals. Further, the rule also limits the types of restrictions that an individual can impose on the medical data. The privacy rule states that the CEs must protect PHI irrespective of how they are generated by implementing safeguards to prevent their improper disclosure. It further obligates all the covered entities to provide training to all their workforce members to ensure compliance with HIPAA privacy rules [21].

The HIPAA security rule complements the privacy rule and provides recommendations for the implementation of *administrative*, *physical*, and *technical* safeguards by covered entities to ensure the availability, confidentiality, and integrity of all *electronic health records*. The administrative safeguards recommends 1) implementation of policies and procedures to prevent, detect, and contain security violations; 2) designation of an individual responsible for managing security; 3) implementation of policies and procedures for ensuring only authorized workforce staff have access to Electronic PHI (EPHI); 4) development of a security awareness and training program for the CE's entire workforce; 5) implementation of policies and procedures for reporting, responding, and managing security incidents; 6) implementation of policies and procedures for disaster and emergency that damages information systems containing EPHI; 7) ensuring all business associates who create, receive, maintain, or transmit EPHI on behalf of the CE will safeguard EPHI [26]. The physical safeguards further recommend 1) implementing policies, procedures, and processes that limit physical access to electronic information systems ensuring authorized access only; 2) implementing procedures that specify appropriate use of data access devices (e.g., PCs, PDAs) and characterize physical environment of workstations that can access EPHI; 3) implementing physical safeguards for all data access devices that can access EPHI in order to limit access to authorized users; 4) implementing policies, procedures, and processes for receipt and removal of hardware and electronic media that contains EPHI in and out of CE and movement of those items within the CE [26]. Finally the technical safeguards include provisions for developing and implementing policies, procedures, and process for electronic information systems, which 1) ensured access control; 2) maintained audit trails; 3) maintained data integrity; 4) enforced authentication; and 5) ensured transmission security [26].

With the development of pervasive healthcare system, and pervasive availability of information, prevention of fraud and abuse will become an ever greater issue. The introduction of HIPAA law provides framework for ensuring the security of medical data, especially the electronic versions, and maintaining patients' privacy. Care needs to be taken to ensure that every pervasive healthcare system maintains the security by implementing comprehensive solutions that are both technically sound and legislatively compliant.

15.4 Conclusions

In this chapter, we presented an overview of security solutions for pervasive healthcare systems. We began by motivating the need for security in pervasive healthcare systems and what are associated challenges. We then presented security solutions for a pervasive healthcare system, starting with the security issues associated with medical sensors, which collect health data from individuals, followed by access control issues that help control the entities that can access EPRs that store the health data in the system. Finally we presented the complementary legislative aspect to providing security in pervasive healthcare systems by discussing the HIPAA security and privacy rules and their provisions for ensuring privacy and security of electronic health data.

15.5 Acknowledgments

This work is supported in part by a gift from Mediserve Inc. and grants #ANI-0196156 and #CNS-0617671 from the National Science Foundation.

Bibliography

1. Upkar Varshney, Pervasive Healthcare, *IEEE Computer*, Vol. 36, No. 12 (2003), pp. 138–140.
2. For the Record: Protecting Electronic Health Information, *National Academy Press*, 1997.
3. S. Cherukuri, K. Venkatasubramanian, and S.K.S. Gupta, BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body, *Workshop on Wireless Security and Privacy (WiSPr)*, International Conference on Parallel Processing Workshops, 2003, Taiwan.
4. Shu-Di Bao and Yuang-Ting Zhang, A New Symmetric Cryptosystem of Body Area Sensor Networks for Telemedicine, *6th Asian-Pacific Conference on Medical and Biological Engineering*, Japan, 2005.
5. Shu-Di Bao, Yuang-Ting Zhang, and Lian-Feng Shen, Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems, *27th IEEE Conference on Engineering in Medicine and Biology*, Shanghai, China, 2005, pp. 2455–2458.
6. Ari Juels and Martin Wattenberg A Fuzzy Commitment Scheme, *ACM Conference on Computer and Communications Security*, 1999, pp. 28–36.
7. K. Van Laerhoven et al. Medical Healthcare Monitoring with Wearable and Implantable Sensors, *The 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications*, Nottingham, U.K., 2004.

8. N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, Security flaws in 802.11 data link protocols. *Commununications of ACM.* Vol. 46, No. 5, May 2003, pp. 35–39.
9. Nikita Borisov, Ian Goldberg, and David Wagner, Intercepting mobile communications: the insecurity of 802.11, *7th Annual Iinternational Conference on Mobile Computing and Networking*, Rome, Italy, 2001, pp. 180–189.
10. Scott R. Fluhrer, Itsik Mantin, and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, *8th Annual International Workshop on Selected Areas in Cryptography*, pp. 1–24, 2001.
11. V. Stanford, Pervasive Health Care Applications Face Tough Security Challenges, *IEEE Pervasive Computing*, Vol. 8, No. 12, April-June 2002.
12. Alfred C. Weaver, Biometric Authentication, *IEEE Computer*, Vol. 39, No. 2, pp. 96–97, Feb 2006.
13. U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, Biometric cryptosystems: issues and challenges, *IEEE Special Issue on Enabling Security Technologies for Digital Rights Management*, Vol. 92, No. 6, June 2004, pp. 948–960.
14. K. Fishkin and J. Lundell, RFID in healthcare, *RFID: Applications, Security, and Privacy, S. Garfinkel and B. Rosenberg*, Ed. Addison-Wesley, 2005, pp. 211–228.
15. Yanjiang Yang, Xiaoxi Han, Feng Bao, R.H. Deng, A smart-card-enabled privacy preserving E-prescription system, *IEEE Transactions on Information Technology in Biomedicine*, Vol. 8, No. 1, pp. 47–58, March 2004.
16. E.S. Hall, D.K. Vawdrey, C.D. Knutson, and K. Archibald, Enabling remote access to personal electronic medical records *IEEE Engineering in Medicine and Biology Magazine*, Vol. 22, No. 3 pp. 133–139, May-June 2003.
17. Alvin T.S. Chan, J. Cao, Henry Chan, and Gilbert Young, A Web-Enabled Framework for Smart Card Application in Health Services, *Communications of the ACM*, Vol. 44, No. 9, September, 2001, pp. 77–82.
18. Jason Reid, Ian Cheong, Matthew Henricksen, and Jason Smith, A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems, *8th Australasian Conference on Information Security and Privacy (ACISP 2003)*, pp. 403–415, 2003, Wollongong, Australia.
19. S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian, Criticality Aware Access Control Model for Pervasive Applications, *4th IEEE Conference on Pervasive Computing (PERCOM)*, Pisa, Italy, 2006.
20. Junzhe Hu and Alfred C. Weaver, A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications, *Pervasive Security, Privacy and Trust (PSPT2004)*, Boston, MA, August 2004.
21. Samuel J. Dwyer III, Alfred C. Weaver, and Kristen Knight Hughes, Health Insurance Portability and Accountability Act, *Security Issues in the Digital Medical Enterprise, Society for Computer Applications in Radiology*, 2nd edition, April 2004.
22. R. Sandhu, E.J. Coyne, H.L. Feinstein and C.E. Youman, Role Based Access Control Models, *IEEE Computer*, Feb 1996, pp. 38–47.
23. D.F. Ferraiolo and D.R. Kuhn, Role Based Access Control, *15th National Computer Security Conference*, 1992.
24. Fundamentals of Mobile and Pervasive Computing, Frank Adelstein, Sandeep K.S. Gupta, Golden G. Richard III, Loren Schwiebert, *McGraw-Hill*, December 2004.
25. R. Clark, e-Consent: A critical element of trust in e-business, *15th Bled Electronic Commerce Conference*. e-Reality: Constructing the e-Economy—Research Volume, 2002.

26. Health Insurance Portability and Accountability Act: Security Rule, www.securityfocus.com/infocus/1764.
27. Unified Authentication Tokens. http://www.verisign.com/products-services/security-services/unified-authentication/index.html/.
28. Mediline Plus Medical Encyclopedia, *U.S National Library of Medicine*, http://www.nlm.nih.gov/medlineplus/encyclopedia.html.
29. L. Biel, O. Pettersson, L. Philipson, and P. Wide, ECG Analysis: A New Approach in Human Identification, *IEEE Transaction on Instrumentation and Measurement*, Vol. 50, No. 3, June 2001, pp. 808–812.