Enhancing the Security of Mobile Health Monitoring Systems through Trust Negotiations

Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung
School of Computing and Mathematics
University of Western Sydney
Sydney, Australia

***Abstract*— There are clear advantages in using remote monitoring systems for elderly care. They help with improving the efficiency in providing higher quality of care. These systems collect relevant data and transmit them to the healthcare provider, to be stored on their servers in the form of patients' Electronic Health Records (EHRs). The EHR may then be used by healthcare professional, either at provider locations or remotely through mobile devices. Among of the main concerns in acceptance of these systems, ensuring the privacy of personally sensitive information and securing EHRs during the transmission can be named. This paper, reports a trust negotiation approach that we have developed to address these concerns. It complements the strengths of the Transport Layer Security (TLS) as the underlying protocol. This combination results in significant improvements in overcoming security related concerns compared to the traditional identity-based only access control techniques. We also report the experimental works that demonstrate the ease of application of the proposed approach in typical mobile environments.**

Keywords-trust negotiations; e-health security; remote health monitoring; mobile application; TLS protocol

I. INTRODUCTION

Remote health monitoring technology is presented as a possible solution for monitoring patients at home. The key issue is to achieve higher quality of care and reduce the cost on patients and governments without affecting the quality of services provided [1]. The use of the remote monitoring system could allow biomedical signals to be measured without the individual's awareness [2]. These researches also show that the homes of the elderly are the best places to collect the medical data and signals related to their bodies, such as their heart rates. There are also benefits associated with improving the quality of care and services, such as reliability, accessibility, frequency, accuracy and availability.

However, it is important to note that precise data measuring techniques need to be used as the healthcare professional will recommend treatment based on the analysis of the data sent by the remote monitoring system. Another important consideration is that the exposure and exchange of this information is faced with the threat of being intercepted, analyzed or even modified as their communications is via unsecured networks. This process will lead to security and privacy concerns related, but not limited, to the confidentiality of patients and to the integrity of the data exchanged. To achieve these security requirements, some improvements to existing protocols, resulting in what is referred to as Ubiquitous Health Trust Protocol (UHTP) is proposed in Section II. UHTP combines trust negotiations with the strengths of Transport Layer Protocol (TLS). The combined approaches, discussed in Section III, ensure that patients' EHRs are only disclosed to the authorized healthcare professionals, on the registered devices and at the authorized locations. For verification purposes, a mobile application is also constructed. Its structure and development are presented in Section IV. The experimental works confirm that by applying UHTP, significant improvements in the security of the remote health monitoring systems can be achieved. The last section gives the conclusions.

II. UBIQUITOUS HEALTH TRUST PROTOCOL

Ubiquitous Health Trust Protocol (UHTP) combines three levels of authentications: Authenticating the healthcare professional, the device in use and the environment of access, referred to as trust negotiation approach, with TLS version 1.0.

Trust is a very complex concept and has a number of different characteristics. Trust negotiations can have different levels which range from simple to advance based cryptographic approaches [3]. It refers to the process of exchanging digital credentials between the client and server for the purpose of authenticating healthcare professionals to the healthcare provider server in remote health monitoring systems. It is a process of establishing trust between two negotiating entities based on their credentials (attributes).

Trust negotiations in e-health have been proposed before, for instance see [4]. The main purpose of such implementations, relate to improving the scalability of the healthcare system. Trust negotiations have also been suggested as a way of establishing a secure session between strangers [5]. Generally speaking, the current security approaches have a strong, albeit sometime implicit, association with the notion of trust. We trust the certificate authority, CA in verifying the digital certificate. In this closed static environment, the interaction between involved entities, organization, CA and the users, is based on trust [6]. However, in ubiquitous computing the role of trust is more highlighted. This is because a UC system, such as ubiquitous monitoring system, involves spontaneous interactions between parties in a decentralized network. In this work, trust negotiations are combined with the well established strong points of the TLS protocol on a mobile application. More specifically, as shown in Fig. 1, trust negotiations are only permitted to occur, after the establishment of the TLS session. This approach guarantees that trust negotiations are actually processed over a secure communication channel. It guarantees the security of the digital credentials exchanged between the client and server. Also, the

978-1-61284-928-7/11/$26.00 ©2011 IEEE

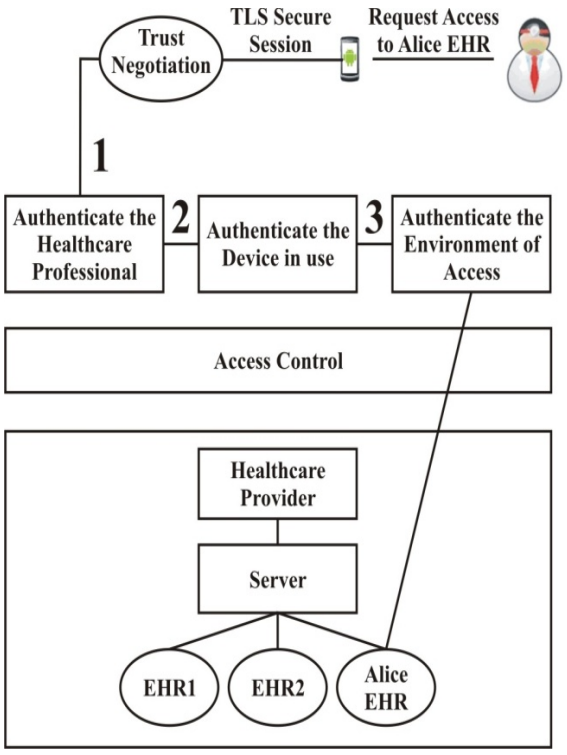

Figure 1. Remote monitoring system.

main goal of extending TLS is to make access control decisions based on attributes rather than on identity. This presents a solution for a distributed environment, where identity based solutions are not enough. A person's (client's) attributes can be in the form of a job title, annual salary, citizenship or others; while server attributes can include privacy policy, role, membership and others. Digital credentials encapsulate the attribute information, described above. They act as a reliable carrier for these attributes. One of the important features of digital credentials is that they are verifiable by the issuer attribute authority. Also, these credentials are treated as protected resources since the information they hold is considered to be sensitive. Credential disclosure is usually controlled by an access control policy. These policies contain instructions and information about the entities which have the right to disclose or access the credentials.

To demonstrate how UHTP operates, the following scenario will be used as a representative example. Bob is a healthcare professional. He is responsible for monitoring a group of five elderly persons which includes Alice. One day, Bob had to visit Alice's home to perform a regular medical examination. To do that, Bob uses the application installed on his mobile device to remotely access Alice's EHR. Using his mobile device, Bob can access and update Alice's EHR, or write any additional notes on the system. However, for Bob to be able to login to the system three conditions must first be met. Firstly, Bob must provide a correct username and password. Secondly, Bob must use a registered mobile device and SIM card. Finally, Bob must be present within an appropriate range, say within 20 meters, of Alice's home location or other authorized location.

III. TRUST NEGOTIATIONS.

The three conditions specified in the scenario given in the previous section, set the three levels of authentication which form the trust negotiation approach. Therefore, the use of a username and password is an application of the first level of trust negotiations, which aims to verify the healthcare professional to the healthcare provider server. In this process both negotiators are assumed to know the requirements necessary for requesting/granting access to patients' EHRs. Therefore, the healthcare provider's server will be expecting to receive the username and password of the healthcare professional when requesting access to EHR. The server must also be configured to receive and support this request.

Only allowing Bob, the healthcare professional, to remote access Alice's EHR using his registered mobile device and his SIM card, is an implementation for the second level of trust negotiations, which relates to authenticating the device in use by Bob. In this level, trust negotiations proceeds into authenticating the mobile device used by the healthcare professional. The process of authenticating the device in use runs silently in the background without the user interference. Authenticating the device in use requires the exchange of digital credentials related to the device itself. They allow a particular device to be identified among others. The International Mobile Equipment Identity (IMIE) number is an example of a digital credential that can be used to identify one mobile device from another. IMIE is a unique number used for identifying mobile devices.

The same requirements used for authenticating the healthcare professional also apply in authenticating the device in use. The server must be configured to request these digital credentials and must know the list of authorized mobile devices. This will allow the server to compare between the received digital credentials and the pre-registered list of digital credentials stored in the server.

Analyzing and comparing these credentials enables the server to make a decision of whether or not to authenticate the device. Restricting access to Alice's EHR from within the range of a certain registered location is an implementation of the third level of trust negotiations, authenticating the environment of access. The environment of access is the location of the healthcare professional at the time where access to EHR was originally initiated. Verifying the environment of access is the last step in the trust negotiation process which needs to be achieved. The successful completion of the trust negotiation approach guarantees that patients' EHR were trusted to the appropriate device, at the right place and received by the authorized person. Yet, authenticating all these players is not sufficient for the release of patients' EHR. There is still a need to meet the rights and policies enforced on the server for the purpose of controlling access to EHR. Therefore, in verifying the environment of access, we check if a particular healthcare professional is located at the monitored person's location performing a medical examination or other healthcare activities. First, we need to get the location where access to EHR has been initiated. Second we need to check if the

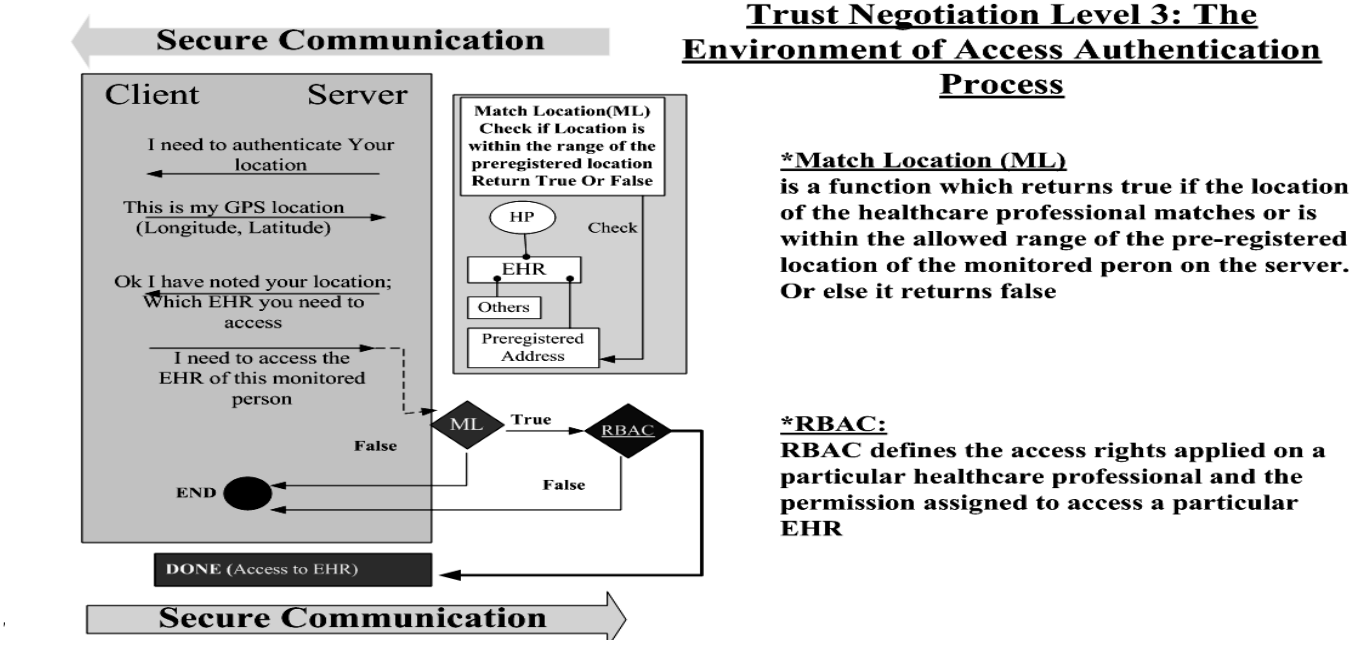

Figure 2. Trust Negotiation Level 3.

location corresponds to the monitored person's pre-registered address on the server. Hence, the monitored person's location must be known to the server prior to the deployment of the remote monitoring system, as well. This process of verification is achieved through the use of a 'Match Location (ML)' function illustrated in Fig. 2. Verifying the location of the healthcare professional is made by verifying the GPS longitude and latitude parameters of the device in use. The longitude and latitude are the digital credentials exchanged between the client and the server. If the function ML returned true, Level 3 of trust negotiations proceeds into checking RBAC access rights. RBAC defines the access rights applied on a particular healthcare professional and the permission assigned to access a particular EHR. RBAC works by controlling the healthcare professionals' access to EHR based on their roles and the permission attached. As an example: after identifying a particular healthcare professional, the server will be able to identify whether this healthcare professional is a doctor, nurse or someone else. Therefore, granting access to a particular EHR will be based on this process of identification. These three levels of authentication, executed within a TLS session, are necessary for the successful completion of UHTP.

IV. The Mobile application and its development

UHTP is implemented as part of a mobile application, the App, which runs on the Android operating system. The App consists of two parts, namely a client side application and a server side application. The first part is developed using the Android SDK [7], the Java Development Kit (JDK) [8] and the Eclipse framework [9]. The client side application generates the user requests and receives and processes the responses sent from the server. The server side application generates the server responses and requests. It holds the patients' EHRs.

This server side application is implemented using the Hypertext Preprocessor (PHP) [10] and JavaScript Object Notation (JSON) [11]. Establishing the trust negotiation process between the client and the server requires the implementation of a server API. This API acts as a web service. It manages incoming messages from the client and outgoing messages from the server, as illustrated in Fig. 3. This is achieved by using the HTTP request methods. That is, the API re-uses the messages and the methods already defined by HTTP, such as the method HTTPPost. In the scenario discussed in Section II, when Bob clicks on the login to your account button from the application, a secure TLS session is created. A sample screenshot is shown in Fig. 4. Bob proceeds by entering his username and password. The trust negotiation process starts immediately after this secure TLS session is established. The next step is for the client side application to send the digital credentials to the server and wait for a response. The digital credentials sent to the server are in the form of an array. Even though Bob has only submitted his username and password, this array also holds the digital credential of the environment of access and the

TABLE I. Array codification

1.	List<NameValuePair> nameValuePairs = new ArrayList<NameValuePair>(6);
2.	nameValuePairs.add(new BasicNameValuePair("username", usernameString));
3.	nameValuePairs.add(new BasicNameValuePair("password", passwordString));
4.	nameValuePairs.add(new BasicNameValuePair("serial", simSerialFinal));
5.	nameValuePairs.add(new BasicNameValuePair("IMIE", imeiFinal));
6.	nameValuePairs.add(new BasicNameValuePair("longitude", loc.getLatitude()));
7.	nameValuePairs.add(newBasicNameValuePair("latitude", loc.getLongitude()));
8.	httppost.setEntity(new UrlEncodedFormEntity(nameValuePairs));

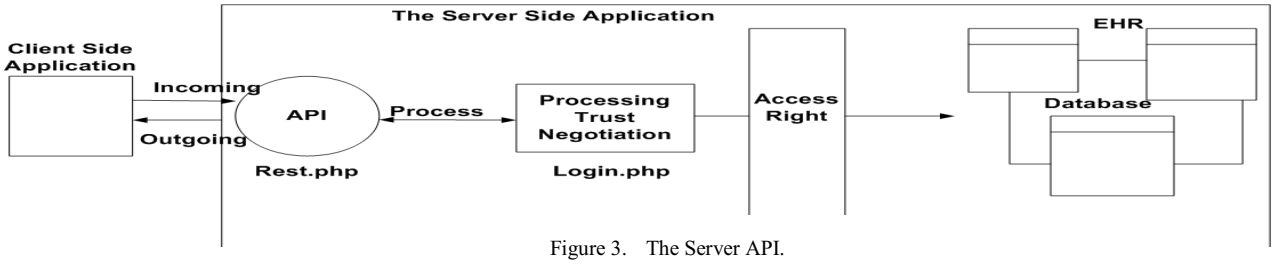

Figure 3. The Server API.

device in use. The code for this array is given in TABLE I. In this array, entries 2 to 7 hold the following six items: username, password, Serial, IMIE, longitude and latitude. The username and the password are Bob's, the healthcare professional digital credentials. The serial is the serial number of Bob's SIM card and the IMEI is the International Mobile Equipment Identity of Bob's mobile device The IMEI and the SIM serial numbers are unique. These numbers are preregistered on the server as belonging to Bob. They are used to identify Bob's mobile device. Therefore, in order for Bob to authenticate his mobile device, he must be using his own mobile device and his own SIM card. The longitude and the latitude, statement number 6 and 7 from TABLE I, represent Bob's GPS location. A GPS location is determined using these two attributes. They are used to authenticate the environment of access. When Bob requests access to Alice's EHR, the server compares Bob's GPS location with the preregistered location of Alice to see if Bob is in the allowed range of access. Authenticating the environment of access is made based on this comparison. Therefore, the client is authenticated to the server when the server verifies the digital credentials included in the array sent by the client. The process of verification is made on the server by extracting the values from the array and by performing the three levels of authentication of the trust negotiation approach. If verification fails, the server generates a server response code '401' and sends it to the client side application. The server API transforms the response code '401' into a readable message to Bob which is 'unauthorized login'. If verification succeeds, it means the three levels of authentication are completed. Next, UHTP checks if Bob has the sufficient rights to access Alice's EHR, before granting him access to her EHR.

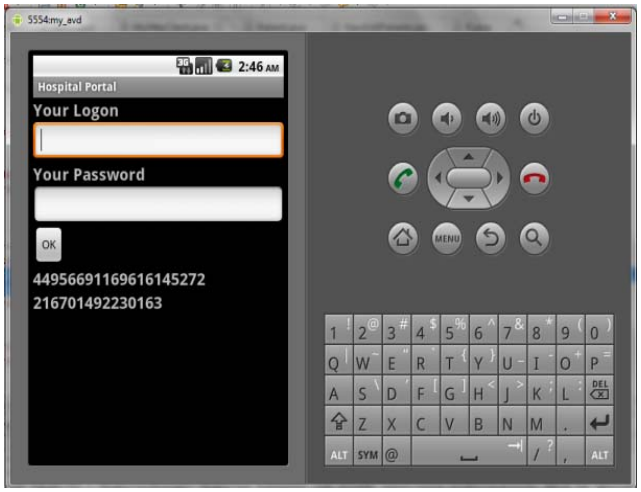

Figure 4. The application shortcut.

V. CONCLUSIONS

In this paper a number of security requirements for remote access to patients' EHR have been considered. As with other secure systems, authorization of healthcare professionals before granting to patients' EHR is an obvious requirement. Others security requirements that must be addressed relate to the vulnerabilities of the mobile devices to their loss and theft. The approaches proposed in this work address these issues. They build on using the strengths of existing approaches to secure the transmission of data over unsecure networks, such as the Internet. Moreover, they address the security and privacy concerns for access to patient data using mobile devices. They ensure that patients' EHRs are only disclosed to the authorized healthcare professional, using registered devices and at authorized locations. Our future works will expand these, to cohesively address collection, storage and transmission of patient data in an efficient and secure manner, intended for users who are not necessarily security experts.

REFERENCES

[1] A. Yamazaki, A. Koyama, J. Arai, and L. Barolli, "Implementation and Evaluation of a Ubiquitous Health Monitoring System," in *Complex, Intelligent and Software Intensive Systems, 2009. CISIS '09. International Conference on*, 2009, pp. 367-374.

[2] J. M. Choi, *et al.*, "A System for Ubiquitous Health Monitoring in the Bedroom via a Bluetooth Network and Wireless LAN," in *Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE*, 2004, pp. 3362-3365.

[3] K. Seamons, "TrustBuilder: Automated Trust Negotiation in Open Systems," presented at the 3rd Annual PKI R&D Workshop, Gaithersburg- Brigham Young University, 2004.

[4] D. K. Vawdrey, T. L. Sundelin, K. E. Seamons, and C. D. Knutson, "Trust negotiation for authentication and authorization in healthcare information systems," in *Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE*, 2003, pp. 1406-1409 Vol.2.

[5] N. Asokan and L. Tarkkala, "Issues in initializing security," in *Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on*, 2005, pp. 460-465.

[6] Z. Liu and D. Xiu, "Agent-based Automated Trust Negotiation for Pervasive Computing," presented at the Proceedings of the Second International Conference on Embedded Software and Systems, 2005.

[7] SDK., *Android SDK*. http://developer.android.com/sdk/index.html

[8] *Java Development Kit (JDK)*. http://java.sun.com/products/archive/jdk/1.1.8_010/

[9] Eclipse - *The Eclipse Foundation open source community website.* http://www.eclipse.org/

[10] *PHP: Hypertext Preprocessor*. www.php.net/

[11] *JSON*. www.json.org