IMPROVING E-HEALTH SECURITY THROUGH TRUST NEGOTIATION

Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung
School of Computing and Mathematics, University of Western Sydney
Locked Bag 1797, Penrith South, DC NSW 2751, Australia

Keywords: Trust Negotiation, e-health Security, Remote Health Monitoring, Mobile Application, TLS Protocol.

Abstract: To achieve higher levels of efficiency and to improve the quality of care, remote monitoring systems for elderly offer interesting solutions. The data collected by the monitoring system are transmitted to the healthcare provider and stored on the healthcare provider's server in the form of patients' Electronic Health Records (EHR). It is important to secure the transmission of the patient's EHR between the healthcare provider server and the mobile device being used by the healthcare professional, as their communication is normally via unsecure networks, such as the Internet. The approaches proposed in this study ensure that patients' EHRs are only disclosed to the authorized healthcare professionals, on the registered devices and at the appropriate locations. To achieve these security requirements, building on the strengths of Transport Layer Security (TLS) protocol, a trust negotiation approach is proposed. For verification purposes, a mobile application is also constructed. The experimental works confirm that by applying the proposed approach, significant improvements in the security of the remote health monitoring systems can be achieved.

1 INTRODUCTION

Elderly remote monitoring systems offer interesting solutions and improve the quality of care. A remote health monitoring system provides platform assistance to the elderly in their homes or other monitored locations. Monitoring patients can help with early detection of problems and can increase their chances of survival. It will also help healthcare providers to react before a serious medical condition, such as a heart attack or diabetic emergency occurs (Kim et al., 2010). There are other associated benefits from the use of remote health monitoring systems specifically for people who live in remote locations or are too ill to visit hospitals or medical offices. Although, a remote monitoring system is an opportunity for improving the healthcare sector; there are a number of limitations involved. In order for this technology to become feasible, challenges exist. These challenges relate to the deployment of this technology and to issues, such as resource constraints, user mobility, cost, heterogeneity of devices, scalability, security and privacy. The proposed approaches in this study address the security and privacy issues generated from the use of remote health monitoring systems. They ensure that patients' EHRs are only disclosed to the authorized healthcare professionals, on the registered devices and at the appropriate locations. Also, they ensure the confidentiality of information by securing its transmission, using Transport Layer Security (TLS) as the underlying protocol. Building on the strengths of this protocol, a trust negotiation approach is developed in section 2. In section 3, the proposed approaches are developed in a mobile application which demonstrates the achievement of the identified security requirements. Trust negotiation is the term used for exchanging the digital credentials between a client and server for the purpose of authenticating healthcare professionals to the server in remote health monitoring systems. It is a process of establishing trust between two negotiating entities based on their credentials. Trust negotiation can be based on different approaches: simple, trial informed and advanced (Seamons, 2004). In e-health security, trust negotiation has been previously addressed. The purpose behind its usage is to improve the scalability of the healthcare system, by enhancing the authentication and access control mechanisms (Vawdrey et al., 2003). In another research, trust negotiation method is used to establish a secure session between strangers (Asokan

Elkhodr M., Shahrestani S. and Cheung H..
IMPROVING E-HEALTH SECURITY THROUGH TRUST NEGOTIATION .
DOI: 10.5220/0003613701720177
In *Proceedings of the 6th International Conference on Software and Database Technologies* (ICSOFT-2011), pages 172-177
ISBN: 978-989-8425-76-8

and Tarkkala, 2005). Users, in this study, enter an ad hoc network and provide authentication through the use of a digital certificate; which authenticates them and their access devices. However, this model is only considered suitable for a small scope authentication system. Other studies, introduced Dynamic Trust Negotiations (DTN) which aims at establishing trust between strangers (Ajayi et al., 2007). This trust is achieved through the use of intermediate trusted entities. Iterative exchange of credentials method is also used to establish a mutual trust between the negotiating parties (Han et al., 2009). This process is referred as automated trust negotiation. Automated trust negotiation is based on what an entity has and does not rely only on the person's identity.

2 TRUST NEGOTIATION

For creating secure sessions, the TLS protocol is used. TLS renders security for communication covering networks, typically the Internet. It enciphers the sections of network connections at the application layer in order to guarantee end-to-end communication at the transport layer. The TLS Protocol can be extended to include trust negotiation; which enhances the security of this protocol. The extension process makes access control decisions based on attributes rather than on identities. This presents a solution for distributed environments, where identity based solutions are not enough. A person'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. To enhance the security of remote monitoring systems, Ubiquitous Health Trust Protocol (UHTP) is presented. This protocol combines trust negotiation with the TLS version 1.0 protocol. UHTP establishes a secure session, using the TLS handshake, between the healthcare professional's mobile device and the healthcare provider's server. Building on the strengths of the TLS protocol, a trust negotiation approach is developed. This approach authenticates the person receiving the care, the person administering it, the mobile device used in accessing the health information, as well as the location where the healthcare is administered. This ensures that patients' EHRs are only disclosed to the authorized healthcare professionals, on the registered devices and at the appropriate locations. These are the three levels of verification performed in this approach as shown in figure 1.

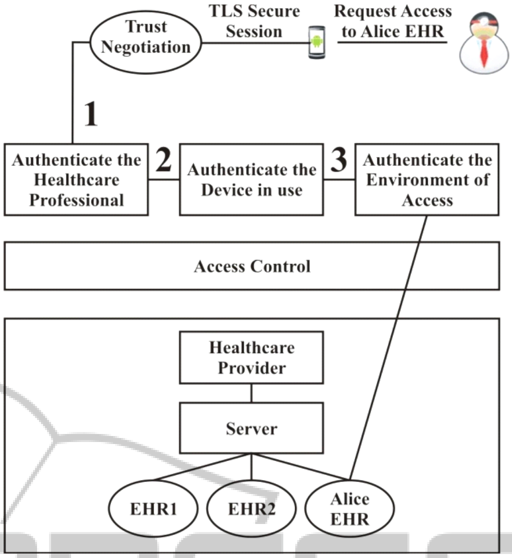

Trust Negotiation
TLS Secure Session
Request Access to Alice EHR
1
Authenticate the Healthcare Professional
2
Authenticate the Device in use
3
Authenticate the Environment of Access
Access Control
Healthcare Provider
Server
EHR1
EHR2
Alice EHR

Figure 1: The Three Levels of Trust Negotiation.

2.1 Authenticating the Healthcare Professional

This level 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, these are the steps 1 to 4 shown in figure 2. The server must also be configured to receive and support this request. Digital credentials are the attributes exchanged between the client and the server for the purpose of verification. It encapsulates the credentials being exchanged; in this case the username and password.

In UHTP, providing the identity of the healthcare professional is not enough to be granted access to EHR, access to EHR is only granted after the completion of the three levels of authentication and after verifying access control rights applied on the server. Figure 2 details the process of authenticating the healthcare professional to the server.

2.2 The Device Authentication

In this level, trust negotiation proceeds into authenticating the mobile device used by the health-care 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

```
Trust Negotiation- Start
Start TLS Session:
   1-  Server → Client: Finish (encrypted)

Start trust negotiation Level 1- Healthcare Professional Authentication
   2-  Client → Server: ClientHello Begin trust negotiation process
   3-  Server → Client: SeverHello
   4-  Digital Credentials
      4.1Client → Server: Digital Credentials (Username and Password). Move to
         Step 5
      4.2Nothing sent from client:
         Server → Client: Session expires. End trust Negotiation

UHTP Server Verification:
   5-  Server: Username check
      5.1  Username found then proceeds to Step 6
      5.2  Else: Server → Client: Unauthorized login; move to Step 7
   6-  Server: Password check
      6.1  Password corresponds to username then proceeds to Step 8
      6.2  Else: Server → Client: Unauthorized login; move to Step 7

End of Server Verification
   7-  Server: Unauthorized login
      7.1  Server → Client: Halt()
      7.2  Server → Client: move back to Step 3
   8-  Server: Proceed1(). Start Level 2 of trust Negotiation
End Level 1
```

Figure 2: Level 1 of Trust Negotiation

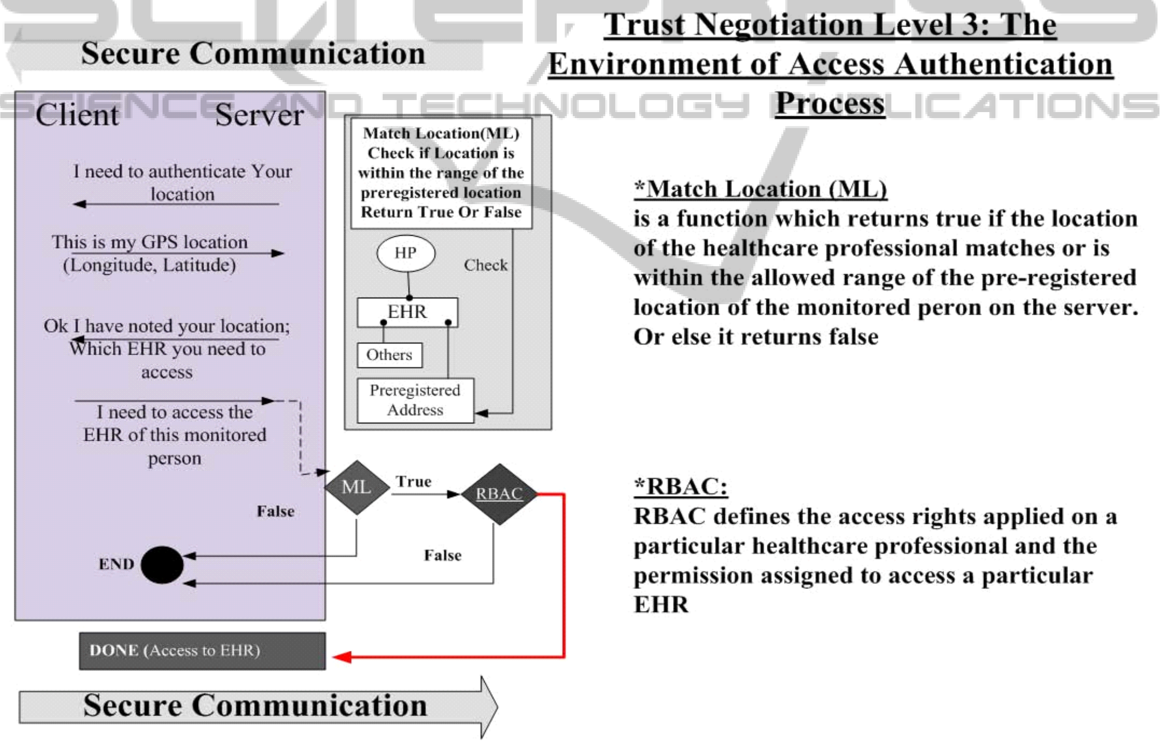
related to the device itself this time. The digital credentials can be in the form of attributes related to the device. They allow a particular device to be identified among others. The International Mobile Equipment Identity (IMIE) number is an example of a digital credential that can be used to identify 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. This process of authentication is given in figure 3. In Step 3 the client send the device in use's digital credentials which are the Mobile IMIE and the SIM serial numbers to the server for the purpose of authenticating the device in use.

2.3 The Environment of Access Verification

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 present at the monitored person's location. The assumption is that this healthcare professional is located at the monitored person's location performing a medical examination or other healthcare activities. Thus, access to the monitored patient's EHR is required by this healthcare professional. To achieve this verification, two requirements need to be met. First, we need to get

```
Trust Negotiation- Start Level 2 - Device in use (DU) authentication. Still
within the current TLS session
   1-   Server → Client: Request DU Digital Credentials
   2-   Digital Credentials
      2.1Client → Server: Digital credentials (IMIE and others). Move to Step 3
      2.2(Nothing sent from client)
         Server → Client: Session expires. End trust Negotiation
UHTP Server Verification:
   3-   Server: DU Digital Credential check
      3.1Server: CheckCredential(). If it returns "True"; moves to Step 5
      3.2Else: Server → Client: Unauthorized login; proceeds to Step 4
End of Server Verification
   4-    Server: Unauthorized login
      4.1Server → Client: Halt()
         Server: Proceed 2(). Start Level 3 of trust negotiation.
```

Figure 3: Level 2 of Trust Negotiation.


Trust Negotiation Level 3: The Environment of Access Authentication Process
Secure Communication
Client
Server
I need to authenticate Your location
This is my GPS location (Longitude, Latitude)
Ok I have noted your location; Which EHR you need to access
I need to access the EHR of this monitored person
Match Location(ML) Check if Location is within the range of the preregistered location Return True Or False
HP
Check
EHR
Others
Preregistered Address
ML
True
RBAC
False
False
END
DONE (Access to EHR)
Secure Communication

*Match Location (ML)
is a function which returns true if the location of the healthcare professional matches or is within the allowed range of the pre-registered location of the monitored peron on the server. Or else it returns false

*RBAC:
RBAC defines the access rights applied on a particular healthcare professional and the permission assigned to access a particular EHR

Figure 4: Level 3 of Trust Negotiation.

the location where access to EHR has been initiated. Second, we need to check if the collected 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 Figure 4.

The algorithm for level 3 of UHTP trust negotiation is given in figure 5. For a given location, the healthcare professional can only access the EHR of the monitored persons who are monitored at this particular location. These are the Steps 1, 2, 3 and 4 from the algorithm shown in figure 5. The Match Location (ML) function, through Steps 4 and 5, returns true if the location of the healthcare professional, sent earlier in Step 2, matches or falls

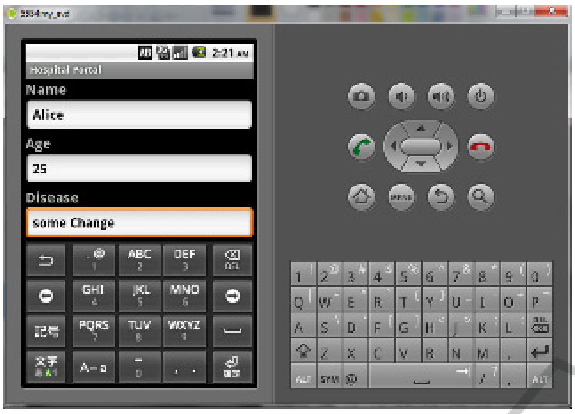
```
Trust Negotiation- Start- Still within the current TLS session
   Proceed2(): Server: Start Level 3
   Start trust negotiation level 3- Environment of Access authentication
   1- Server → Client: Request the environment of access Digital Credentials
   2- Digital Credentials
      2.1 Client → Server: Digital credentials (GPS location). Move to Step 3
      2.2 Nothing sent from Client:
          Server → Client: Session expires. End trust Negotiation
   3- Request access to a particular EHR:
      3.1 Client → Server: request access to the EHR of a particular monitored
          person. Move to Step 4
      3.2 Nothing sent from Client:
          Server → Client: Session expires. End trust Negotiation
UHTP Level 3 Server Verification:
   4- Match Location function: Server: ML()
      4.1 (If True) Server: Move to Step 6.
      4.2 (If false) Server: Move to Step 5
   5- Server: Unauthorized login
      5.1 Server → Client: Halt()
   6- Server: RBAC().
      6.1 (If True) Server: Assign role, permission. Move to Step 8.
      6.2 (If false) Server: Move to Step 7
   7- Server: Unauthorized login
      7.1 Server → Client: Unauthorized access (No permission to access
          resource)
      7.2 Server: Move back to Step 3.
   8-Server → Client: Done()
```

Figure 5: Trust Negotiation Level 3 Algorithm.

within the allowed range of the pre-registered location of the monitored person. In case the verification of the location fails, the ML function returns false (Step 4.2) and trust negotiation fails. 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 negotiation 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 are the Steps 6 and 7 shown in figure 5.

3 THE EXPERIMENTAL RESULTS

Ubiquitous Health Trust Protocol (UHTP) was implemented as part of a mobile application which runs on the Android operating system, as shown in Figure 6. The application (the App) is modelled in terms of a client and server architecture wherein a client requests information from a server. The server typically responds with the requested information. Implementing trust negotiation on the server required the implementation of a server API. This API acts as a web service. It has the responsibility of handling incoming messages from the client and outgoing messages from the server. This is achieved by using the HTTP request methods. Therefore, the API re-uses the messages and the methods already defined in the HTTP protocol, such as the method HTTPPost. For instance, this method is used to send the username and password of the healthcare professional, the mobile IMIE and the SIM serial numbers as well as the location parameters (the GPS



Hospital Portal

Name

Alice

Age

25

Disease

some Change

Figure 6: The App’s screen shot.

longitude and latitude) to the server. The server API also has the responsibility of reading and parsing the client’s message and responding accordingly.

To remotely access the EHR of a particular monitored person, the healthcare professionals use the App installed on their Android mobile devices and enter their usernames and passwords to logon to the App. Subsequently, the App carries out, in a transparent manner to the healthcare professional, the UHTP trust negotiation process; which involves the three levels of authentication previously described. It silently performs the authentication process within a secure session. This guarantees the encryption of the messages exchanged between the client and the server. If trust negotiation succeeds and the healthcare professional has sufficient rights to access the requested EHR, then access will be granted. This application was tested to be fully functional running on an Android mobile device emulator. It can be installed on a wide range of mobile devices running Android as an operating system. It can also operate on wireless connections and mobile infrastructure. This application has demonstrated the successful integration of trust negotiation and the TLS protocol. These experimental works confirm that by applying the proposed trust negotiation approach, the expected analysis results can be achieved. The developed application is also practical and easy to adopt, as users are not required to have any additional knowledge or expertise in the use of the underlying technologies. The results collected from this experiment show significant improvements in overcoming security concerns. The improvements in the security of the remote monitoring systems are achieved by providing extra protective features to the access control and authorization process before the release of any data over unsecured network.

4 CONCLUSIONS

The approaches proposed in this study ensure that patients’ EHRs are only disclosed to the authorized healthcare professional, on the registered device and at the appropriate locations. They ensure the confidentiality of information, by securing its transmission, using Transport Layer Security (TLS) as the underlying protocol. Building on the strengths of this protocol, a trust negotiation approach is developed. This approach authenticates the person receiving the care, the person administering it, the mobile device used in accessing the health information, as well as the location where the healthcare is administered. However, this study did not address the security issues arising from the use of the remote monitoring system on the patient’s side. Future research needs to take a more holistic view for elderly health monitoring.

REFERENCES

Ajayi, O., Sinnott, R. & Stell, A. 2007. Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems. In: *Availability, Reliability and Security, 2007 ARES 2007*. The Second International Conference on, 10-13 April 2007 2007. 3-10.

Asokan, N. & Tarkkala, L. 2005. Issues in initializing security. In: *Signal Processing and Information Technology, 2005*. Proceedings of the Fifth IEEE International Symposium on, 21-21 Dec. 2005. 460-465.

Han, R.-F., Wang, H.-X., Wang, Y.-H. & Zuo, K.-L. 2009. Membership-Based Access Control for Trust Negotiation in Open Systems. In: *Information Assurance and Security, 2009, IAS '09*. Fifth International Conference on, 18-20 Aug. 2009. 189-192.

Kim, J., Choi, H.-S., Wang, H., Agoulmine, N., Deerv, M. J. & Hong, J. W.-K. 2010. POSTECH's U-Health Smart Home for elderly monitoring and support. In: *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010* IEEE International Symposium on a, 2010. 1-6.

Seamons, K. 2004. TrustBuilder: Automated Trust Negotiation in Open Systems. *3rd Annual PKI R&D Workshop*. Gaithersburg- Brigham Young University.

Vawdrey, D. K., Sundelin, T. L., Seamons, K. E. & Knutson, C. D. 2003. 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, 17-21 Sept. 2003. 1406-1409 Vol.2