10

Network security in a telemedicine system

G. Vassilacopoulos, V. Chrissikopoulos and D. Peppes

Department of Informatics, University of Piraeus,
80 Karaoli & Dimitriou Str. 185 34 Piraeus, Greece
tel. : +30 1 4222124
fax : +30 1 4112463
e-mail : gvass@unipi.gr , chris@unipi.gr and pepes@unipi.gr

Abstract

Enforcing network security in Telemedicine systems is necessary in order to ensure security of the information exchanged. In this paper we propose a conference key distribution system that is able to provide the network security services required in an anticipated implementation. The protocol is based on public keys and has a low communication and computation complexity. In addition, a scenario for secure data exchange through the Telemedicine system network based on this protocol is presented.

Keywords

Telemedicine system, network security, cryptographic protocol, conference key

1 INTRODUCTION

Recent years have seen an increasing need for communicating healthcare-related data and telematics development offers the best opportunities. In many cases moving the information instead of the patient is judged sufficient. Telemedicine offers rapid access to shared and remote medical expertise by means of telematics technology no matter where the patient or relevant information is located (Sommer 1994). Thus, telemedicine can be considered as a means towards meeting the strategic challenge of moving the point of care closer to the citizen.

P. Horster (ed.), *Communications and Multimedia Security II*

Telemedicine can offer improved medical care to remote areas for an average patient in an everyday life situation up to very sophisticated methods for diagnosis and therapy planning by transmitting and interpreting multimedia medical data. Hence, the added value of telemedicine for both the health professional and the patient is considerable. For example, the physician of a remote health centre can, in difficult cases, use the available telematics means to discuss clinical information, including images, with another expert (or experts) and because of this facility the patient enjoys better care.

One of the characteristics of telemedicine is the independence of the way of communicating making use of available or developing telecommunication infrastructures. Hence, telemedicine may evolve as an alternative to the current healthcare delivery. However, its cost-effectiveness under the social, economical and other constraints of a particular installation is a problem requiring a thorough evaluation.

One important consideration in a telemedicine system design and implementation is to ensure that security and confidentiality problems of data transmission are tackled effectively (Sommer 1994). This paper deals with this aspect of a telemedicine system implementation and presents a practical and provably secure protocol. The protocol extends the features provided by the protocols proposed in (Burmester-Desmedt 1995, Chrissikopoulos-Peppes 1995, Matsumoto et al. 1986, Yacobi 1991) and can be implemented in cases where two or more parties wish to communicate simultaneously; it has been proposed for implementation into an intended telemedicine installation between the "Gennimatas" General District Hospital of Athens (GGDHA) and its "satellite" health centres situated in remote areas and islands.

2 A TELEMEDICINE SYSTEM REQUIREMENTS

Our basic motivation for this research stems from our involvement in exploring the possibility of implementing a telemedicine system in order to provide improved healthcare services to the citizens of four remote areas covered by health centres that operate as "satellites" (both medically and administratively) to the GGDHA. At first phase, the health centres are intended to communicate directly with the hospital through dedicated data lines upon request for a peer-to-peer consultation with a cardiological expert of the hospital, based on ECG-related data. Figure 1 shows an overall view of the anticipated telemedicine network. At a later stage, it is intended to also transmit static pathology and radiology pictures.

A major concern of the telemedicine exploratory study was to ensure security of the information exchanged through the network. The main security services to be provided were identified as (EEC/DGXII 1991, ISO/IEC 7492-2 1989, Janson-Molva 1991, Pfitzmann-Pfitzmann 1991):

- *Integrity of information.* The exchanged information does not change during the transmission and this information can be modified only be authorized users. In case where the exchanged information is modified, the authorized users have to detect the modification and reject the relevant data.
- *Confidentiality of information.* The exchanged information is only disclosed to authorized users. The information must be maintained secure and private when is transferred through the network.

- *Authentication of users.* The users who communicate have to verify their identity. When a user *A* communicates with a user *B* then user *A* has to ensure that the received information is from user *B* and vice versa.

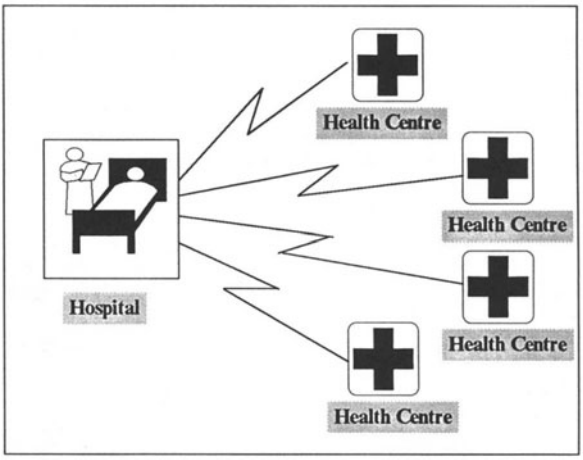

Figure 1 An overall view of the telemedicine network.

However, the level of security that should be included in the systems involves some judgement about the dangers associated with system use and the resource implications of various means for avoiding or minimising those dangers. To this end, a thorough risk analysis is required before the level of security enforcement is decided.

3 A TELEMEDICINE NETWORK SECURITY PROTOCOL

Network security is usually provided through encryption/decryption of the exchanged information (EEC/DGXII 1991, Pfitzmann-Pfitzmann 1991). Security in a telemedicine system network is required to ensure that the patient's medical record (or parts of it) exchanged among the users is protected from such threats as masquerading, data modification or destruction (ISO/IEC 7492-2 1989, Janson-Molva 1991).

As mentioned above, the basic services that a network security system should provide are authentication, data confidentiality and data integrity. In addition to these services, the security system desinged should take into account the telemedicine network requirements of the particular installation. Among these are included:

- *Simultaneous participation in a secure communication by two or more parties.* For example, the physician of a health centre may need expert advise on a patient case by a hospital physician. In this case, the health centre physician and the hospital physician may begin a communication session that may also include other

physicians from the hospital (or other hospitals) if a conference is judged necessary, in order to deal with the particular case.

- *Secure compression.* The use of compression techniques is one of the factors for enabling multimedia technology as only through the reduction of the size of the exchanged data the storage and communication of multimedia data is facilitated (Spyns et al. 1994). All data compression techniques use a key in order to compress and uncompress the data. In addition to the protection of the exchanged information, the telemedicine system network should provide protection of these keys as their publication could result in unauthorized access to the exchanged information. To this end, two options are available : (i) the compression technique creates automatically the key used for compression, and (ii) the compression technique requires from the user to enter this key. In the first option, after completion of the compression procedure the cryptographic protocol has to encrypt the compressed data for protection purposes. In the second option, the key used for data compression should be the same with the key used in the encryption and decryption procedures.

In order to provide these services, a secure communication protocol is required. Although several communication protocols have been proposed in the literature, where the involved users are two or more, most of these are either impractical for implementation or based on heuristic arguments to address their security (Ingemarsson et al. 1982, Koyama-Ohta 1988, Tsujii-Itoh1989, Fischer-Wright 1992, Blundo et al. 1993, Matsumoto et al. 1986, Yacobi 1991). However, provably secure and practical communication protocols have also been proposed (Burmester-Desmedt 1995, Chrissikopoulos-Peppes 1995). In addition to these properties, the protocol proposed in this paper is relatively easy to implement due to its low communication and low computational complexity. The security of this protocol is based on the intractability of the Diffie-Hellman problem (Diffie-Hellman 1976) and extends the features provided by the protocols proposed in (Burmester-Desmedt 1995, Matsumoto et al. 1986, Yacobi 1991).

According to the proposed protocol, a Trusted Centre chooses the security parameters (p, α and q, where p is a prime number, $\alpha \in Z_p$ whose order q is a large - superpolynomial in $|p|$). These parameters are announced to the users registered as network users.

Let N be the number of network users and $U_1, U_2, \ldots, U_n$ ($n \leq N$) be a set of network users that want to generate a common shared key in order to have a secure conference. The value of n may vary between conferences but it needs to be fixed for each conference. In the cases of a user leaving or joining the conference, a new session key needs to be created in order for the conference to remain secure. To avoid the computation overhead involved in these cases it is preferred that the number of participants in the conference has been decided upon in advance as it is often the case in telemedicine systems.

In the first phase of the protocol, each user U_i selects a secret key s_i and registers with the Trusted Centre the value $P_i = \alpha^{s_i} mod p$ as its public key.

In the second phase, each user selects a random number r_i from the set Z_p, computes a value $X_i = a^{r_i s_i} \bmod p$ and sends this value to the other users in the conference. Then, each user is taken in a cycle and computes a value

$$Y_i \equiv \left(X_{i+1}\right)^{s_i}\left(X_{i+1}\right)^{s_i r_i} \Big/ \left(X_{i-1}\right)^{s_i r_i}\left(P_{i-1}\right)^{s_i r_i} \pmod{p}$$

which is also sent to the other users in the conference. The common shared key is computed by a combination of all 5-tuples (P_i, X_i, Y_i, r_i, s_i) as

$$K \equiv a^{s_1 s_2(r_1 r_2 + r_2) + s_2 s_3(r_2 r_3 + r_3) + \ldots + s_n s_1(r_n r_1 + r_1)} \pmod{p}.$$

This key can be computed by every user U_i in the conference since

$$K \equiv K_i \equiv \left(\left(X_{i-1}\right).\left(P_{i-1}\right)\right)^{n r_i s_i} . Y_i^{n-1} . Y_{i+1}^{n-2} \ldots Y_{i-2} \pmod{p}.$$

In the case where the number of the users are two (n=2), each user can compute the second message of the other user by himself, as $Y_1 \equiv P_1^{r_2 s_2} \Big/ X_1^{s_2}$ and $Y_2 \equiv P_2^{r_1 s_1} \Big/ X_2^{s_1}$. Figure 2 shows the conference key distribution system for three communicating users.

The described procedure needs to be executed in the cases where either the users want to communicate at first time or the users want to change the common session key for protection reasons (Schneier 1994). In the second case, the users need to preserve the privacy and secrecy of the common session key in order to use this key in the next session that is carried out among the same users. When the users have in their possession this common shared key, they can use any encryption algorithm to encrypt/decrypt the sensitive information transmitted over a public and insecure channel. For example, a DES-like algorithm can be used (U.S. Department of Commerce 1977).

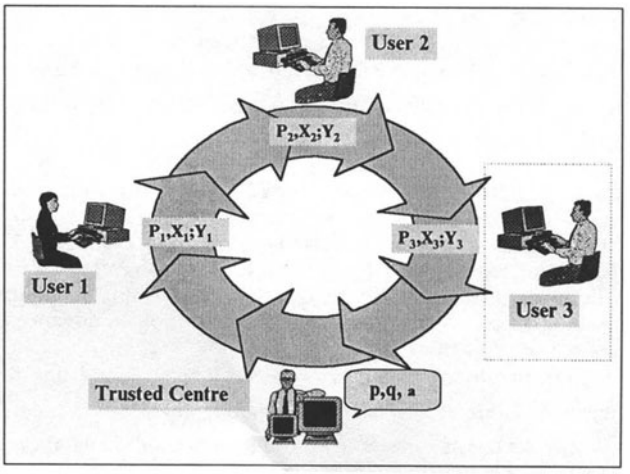

Figure 2 The conference key distribution system for three users.

In the above procedure, the role of the Trusted Centre is restricted to the selection of the appropriate parameters and to the management of the network security system. Thus, the common shared key is derived by the users in such a way that no user can predetermine this key. After the execution of this protocol only an authenticated user can be in possession of the correct key (or in possession of the necessary information to compute the correct key).

4 A PROPOSED IMPLEMENTATION

A scheme for a secure network system based on the cryptographic protocol presented can be established. To this end, there is a need to select a user of the system to play the role of the Trusted Centre. In our proposed implementation at GGDHA the role of the Trusted Centre is assigned to the hospital for the following reasons:

- It has the adequate software, hardware and personnel to provide the assistance necessary at any time.
- It is trusted by every user
- It can maintain (or develop) the necessary applications for the enforcement of the cryptographic protocol into the telemedicine network.

Thus, with regard to security, the following operational scenario of the telemedicine system was proposed:

- *Selection of the parameters.* The Trusted Centre selects and publishes the security parameters of the network security system (i.e. α and p).
- *Registration of the users.* Each network user receives an authorization from the Trusted Centre (i.e. hospital), selects a secret key and computes his/her public key which it registers with the Trusted Centre. This public key has to be distributed to all authorized users or to be stored into a central database (held at the Trusted Centre) accessible by all the authorized users. In either case, the authorized users have only read access to the database of the public keys.
- *Preparation of secure conference.* When there are reasons for a communication session, the relevant user calls the other user(s). At this stage, the procedure described earlier is executed in order to specify a common shared key among the participants.
- *Secure Conference.* When the preparation phase is completed (i.e. the relevant users have a common session key) the conference can begin by using the common session key to encrypt/decrypt the information exchanged among the users. Figure 3 shows a view of a secure conference among three users (two physicians of the hospital and a physician of the health centre) within the Telemedicine network (it is assumed that after computing the common shared key, the conference participants communicate through the telemedicine network).

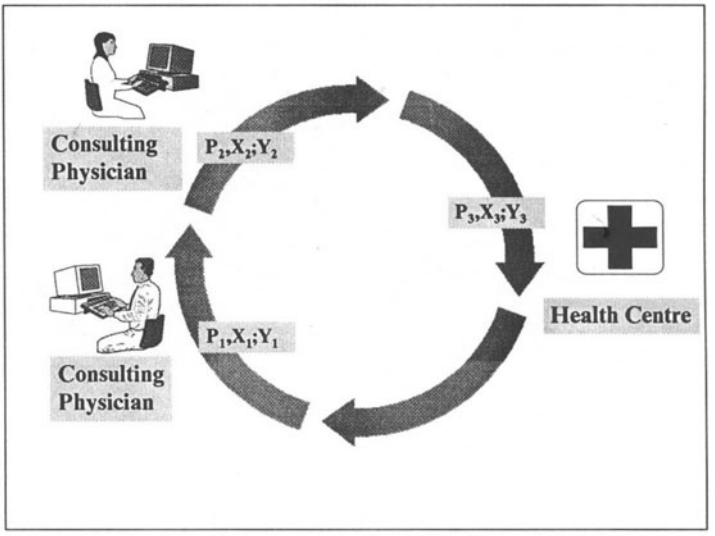

Figure 3 A secure conference within the telemedicine network.

It must be pointed out that in most cases no more than two users will be involved in a telemedicine communication session. However, the proposed protocol will also address the cases where more than two simultaneous users are required to deal with specialized needs of patients. In addition, the protocol can be used within the hospital's high speed (i.e. 100 Mb/s) network in order to enforce security. However, one limitation of the proposed protocol is that each time a session begins or another user is added to an existing communication session the key distribution procedure should start from the beginning (i.e. dynamic key distribution is not supported). This may prove impractical in emergency case situations where rapid communication is required.

5 CONCLUDING REMARKS

A provably secure communication protocol for information exchange within a telemedicine system is proposed. The protocol is based on the intractability of the Diffie-Hellman problem and is practical for implementation due to its low communication, low computational complexity and is independent of the format used to exchange information. It ensures that the users involved can communicate securely since an unauthorized user cannot be in possession of the common shared key (or in possession of the necessary information to compute this key) which the authorized users use to encrypt and decrypt their exchanged information.

6 REFERENCES

Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. (1993) Perfectly-secure key distribution for dynamic conferences. *Advances in Cryptology-Crypto' 92, Lecture Notes in Computer Science #740,* (ed. E. Brickell), Springer-Verlag, 471-487.

Burmester, M. and Desmedt, Y. (1995) A Secure and Efficient Conference Key Distribution System. *Advances in Cryptology-Eurocrypt' 94,* (ed. A. De Santis), Springer-Verlag, 275-286.

Chrissikopoulos, V. and Peppes, D. (1995) A Practical Conference Key Distribution System. *Information Security - the Next Decade, Proceedings of IFIP/SEC'95, The 11th Inter. Information Security Conf.,* (eds. J. Eloff and S. Solms), 168-175.

Diffie, W. and Hellman, M. (1976) New directions in cryptography. *IEEE Trans. Inform. Theory*, **IT-22**, 644-654.

EEC/DGXII, (1991) *Data Protection and Confidentiality in health informatics*, IOS press.

Fischer, M. and Wright, R. (1992) Multiparty secret key exchange using a random deal of cards. *Advances in Cryptology-Crypto' 91, Lecture Notes in Computer Science #576,* (ed. J. Feigenbaum), Springer-Verlag, 141-155.

Ingemarsson, I., Tang, D. and Wong, C. (1982) A conference key distribution system. *IEEE Trans. Inform. Theory*, **28** , 714-720.

ISO/IEC 7492-2 (1989) Information Technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

Janson, P. and Molva, R. (1991) Security in open networks and distributed systems, *Computer Networks and ISND Systems*, **22**, 323-346.

Koyama, K. and Ohta, K. (1988) Identity-based conference key distribution systems. *Advances in Cryptology-Crypto' 87, Lecture Notes in Computer Science #293,* (ed. C. Pomerance), Springer-Verlag, 175-185.

Matsumoto, T., Takashima, Y. and Imai, H. (1986) On Seeking Smart Public Key Distribution Systems. *The Transactions. of the IECE of Japan*, **E69** (2), 99-106.

Pfitzmann, A. and Pfitzmann, B. (1991) Security in Medical Networks. *Data protection and Confidentiality in health informatics, IOS press*, 231-248.

Schneier, B. (1994) *Applied Cryptography, Protocols, Algorithms and Source Code in C*, John Wiley & Sons, Inc.

Sommer, T.J. (1994) Telemedicine: a useful and neccessary tool to improving quality of healthcare in the European Union, *Proceedings of the twelfth International Congress of the European Federation for Medical Informatics,* (eds. P. Barahona, M. Veloso and J. Bryant), Lisbon, Portugal, 278-282.

Spyns, P., Renkens, S. and Willems, J. (1994) Data Compression for Medical Report Archiving, *Methods of Information in Medicine,* **33**, 164-169.

Tsujii, S. and Itoh, T. (1989) An ID-based cryptosystem based on the discrete logarithm. IEEE *J. Selected Areas Commun.*, SAC-**8**, 467-473.

U.S. Department of Commerce (1977), National Bureau of Standards, *Data Encryption Standard*, FIPS Publication **46**.

Yacobi, Y. (1991) A key Distribution Paradox. *Advances in Cryptology-Crypto' 90, Lecture Notes in Computer Science #537,* (eds. A.J. Menezes and S.A. Vanstone), Springer-Verlag, 268-273.