Security aspects in telematics applications for clinical radio-oncology

E. NTASIS, K. S. NIKITA, G. MATSOPOULOS
Institute of Communication and Computer Systems
Department of Electrical and Computer Engineering
National Technical University of Athens
9, Iroon Polytechniou Str., Zografos, 15773 Athens, GREECE

Abstract: - The efficiency and the quality of radio-oncology sector can be significantly increased by making use of telematics methods. The radiotherapy planning procedure can be based on digital patient data - acquired from CT / MRI - which are used to form a virtual patient model. This model can be made available at different sites than those of the patient's physical presence via telematics components mainly based on generally available networks. The addition of telematics components to radiation treatment planning systems will allow cooperation of radio-oncology centres, and lead to a significant cost reduction by virtual sharing of extremely expensive devices. Considering that the information, which is communicated between the involved radio-oncology centres is highly confidential and of great importance for the patient's treatment planning, security aspects must be examined in detail. In this paper, data security requirements together with proposed solutions in order to ensure the secure communication among users of radio-oncology centres are presented. Proc.pp..3981-3984

Key-Words: - Telematics; Security; Radio-oncology; Encryption; Access control system; Digital signature.

1 Introduction

As a result of the increasing specialisation of medicine, and the subsequent specialisation of physicians and equipment, which are not available at every health centre or hospital, it became necessary to transport both personnel and patients between locations to provide a reasonable health care service. Taking into consideration that patients and law require increasing levels of quality and efficiency, health care costs are increasing in a way that will not be supportable in a few years. The alternatives to this conveyance are either to invest in more human resources, conventional infrastructure and equipment or to increase the efficiency and quality of the sector, including the use of telematics methods in a wide range of different applications and services.

The situation becomes critical in the field of radiotherapy, where recent advances of methods and techniques make increasing use of high technology imaging and treatment planning systems, and require more specialised knowledge of radiation medicine and physics. Radio-oncology clinics have a severe need for: a) increasing efficiency of existing personnel b) sharing expensive equipment available in geographically separated locations and c) access to expertise located in remote centres

Based on the above considerations, the treatment planning procedure can be based on digital patient data, which are used to form a virtual patient model. This virtual model can be available at different sites than those of patient's physical location and therefore allow cooperation of radio-oncology centres via telematics applications. Thus, efficiency of personnel and operation of radio-oncology centres will be significantly increased, while radiotherapy related costs will be drastically reduced through both, virtual sharing of extremely expensive devices and remote expert assistance/ service [1].

The health care information system for clinical radio-oncology contains many data related directly to identifiable persons, their illnesses and their treatment. The introduction of electronic processing and transferring of such health care information requires a careful analysis of a large number of security aspects. In this paper, the concept of virtual simulation and treatment planning in clinical radio-oncology via telematics applications is presented, with special emphasis on the related data security issues.

2 Problem Statement

In this section, some preliminary information is given, describing the concept of virtual simulation and treatment planning in clinical radio-oncology and the related data security requirements.

2.1 Information exchange

Virtual simulation and treatment planning for clinical radio-oncology requires the exchange of patient related data between different health care institutions/ organisations, such as hospitals, clinics and radio-oncological centres, as well as between departments of the same institution involved into the radio-oncological process.

The medical data transfer between departments involved into the radio-oncological process can be divided into two phases: (a) when providing the "digitised patient" pictures obtained by CT/MRI scans to the treatment simulation system, and (b) when retrieving the patient's treatment planning (contouring of tumour and critical structures, beams' geometry, dose definition) which is then sent back for the real treatment process.

The kind of health care information, which is exchanged between institutions and we are dealing with in terms of security is medical image using the DICOM 3.0 (Digital Image COMmunication) standard protocol [2], as well as treatment planning related data, like accelerator parameters, field sizes and gantry angles. Considering that a number of 100-150 images are needed for every treatment planning and that the size of every image is 512 x 512 pixels, the size of the data received from the CT and transferred through the network is approximately 50-75 Mb.

The telecommunication platforms used are an Ethernet based network for all local communications between different departments of the same institution, and ISDN reserved lines (Basic Rate Access) for communication between different institutions. Thus, we are dealing with LAN-to-LAN interconnections over ISDN. Regarding Europe as a whole and expecting that in the near future all telecommunications standards will converge to the Euro-ISDN protocol first elaborated in 1993 [3], the telematics aspects should be implemented using these standards.

2.2 Data security requirements

The transmission of medical data over networks is a highly security sensitive process and requires suitable techniques to prevent unauthorised access and misuse of data, and to guarantee the patients privacy. In the following, the requirements for secure communication among users of the radio-oncological system are presented for the LAN and the LAN-to-LAN connection (Fig.1), taking into account all three components of security: confidentiality, integrity and authenticity.

2.2.1 Security requirements over LAN

The security requirements identified on the LAN can be summarised as follows:

Authentication of users is very important, as doctors and other professionals accessing confidential information must be verified. In an access control system, a user must act through a log-in process, which asserts the identity of the applicant.

Authorisation of users is defined as the granting of specific rights. To every user of the system certain access rights must be assigned, determining which kind of information one is permitted to read, modify or generate.

Availability satisfies the need of accessing and using the data whenever an authorised entity wishes to do so. The required availability is in our case as high as 12 hours/day, 7 days/week.

Backups are addressed as part of the overall security plan of every institution securing of all data referring to the radio-oncology system.

2.2.2 Security requirements over LAN-to-LAN

The security requirements that have to be fulfilled over the LAN-to-LAN connection are summarised in the following:

Confidentiality defends the privacy of the treated patient. Since the data channels and the intermediate store-and-forward nodes of the message handling system can be "tapped", cryptography methods must be used for the communicated confidential data.

Integrity is of high priority, as changes or damages of the data may result in wrong treatment planning. Any alteration to the content of image or document communicated, on purpose or accidentally, should be detected. The originator of the information can only be held accountable when he is assured that what he has communicated was not changed, or in the case of changes that the recipient should have detected these changes. Accidentally changes are handled by the Euro-ISDN protocol, while intentionally changes are confronted by authorisation and authentication mechanisms on the LAN.

Authenticity of data ensures the fact that medical images have to be "genuine" and is provided by digital signature mechanisms.

Non-repudiation is provided by digital signature and protects the recipient of a message from attempts by the originator to deny having sent the message, or the message with that specific content (e.g. no possibility for a physician to deny a wrong treatment planning that he has designed).

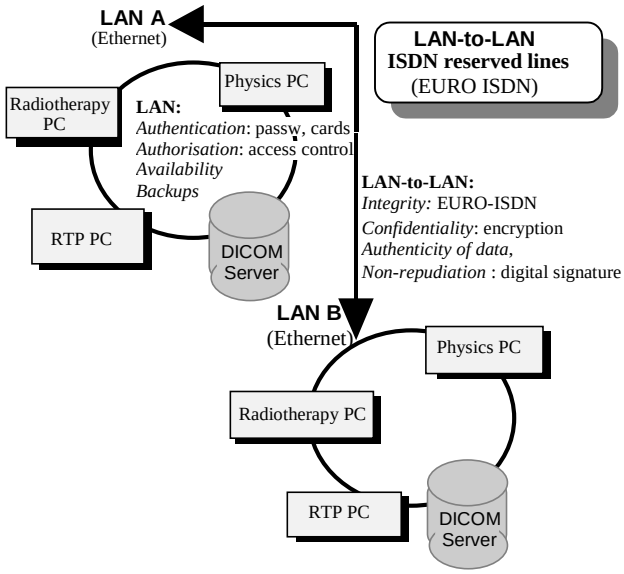

Fig.1 Secure exchange of radio-oncological information

3 Problem Solution

Taking into account the data security requirements over both the LAN and the LAN-to-LAN connection, presented in Section 2.1, in this section, solutions are proposed in order to ensure the secure communication among the users of the virtual simulation and treatment planning system (Fig.1). In this context, an access control system and backups are proposed for secure data exchange over LAN, while cryptography methods and digital signature mechanisms are used in order to provide security over LAN-to-LAN connection.

3.1 Access control system

Authentication of the users is implemented by using an access control system. A user (doctor, physicist) acts through a log-in process, which asserts the identity of the applicant. An individual can prove his claim to identity by what he is (biometric recognition), what he knows (passwords, keys), or by what he possesses (a physical token such as a chipcard) [4]. In the log-in process, the user is prompted to give his name and his password. The password of the users must be kept secret and, in order to prevent or to minimise the effects of a possible password stealing, measures as restricting access to the password file, password ageing, the selection of a password hard to be revealed from impede dictionary attacks and password/account blocking after a predefined number of failed attempts to authenticate, must be taken. An alternative implementation for the log-in process is the use of a chipcard as a more secure way of proving the identity of the user.

The users of the radio-oncological system will be divided by the system security manager in the following groups:

- Medical staff
  - Radiotherapists
- Medical physics professionals
  - Physicists
  - Engineers
  - Dosimetrists
- Special trained technicians
- Treatment radiographers

In order to implement the classification of users into groups, a local security policy (e.g. direction of a hospital, clinic) is consulted and the specific role of the individual in the organisation is determined. The result is a database that maps the identity of a user to a group.

Each group is assigned a number of rights to information objects. As a result, the rights of every user assigned by the system security manager, are determined by the group in which the user belongs. The rights of reading, modifying and generating a document, of every group of users are presented in Table 1.

Table 1. Access rights to radio-oncological system

Users	**Contou-ring PTV**	**Contou-ring CS**	**Beam's Geome-try**	**Dose prescri-ption**	**Norma-lisation**
Medical Staff	r g m	r g m	r g m	r g m	r
Medical physics professionals	r	r g m	r g m	r	r g m
Special trained technicians	r	r g m	r g m	r	r
Treatment radiographers	r	r g m	r g m	r	r

CS: Critical Structure, PTV: Planning Treatment Volumes, r: reading right, m: modification right, g: generation right

3.2 Backups

Backups must be created by every institution and storage must be carefully selected for both its security and its availability. A periodically verification of the correctness and completeness of backups is also necessary.

3.3 Security provided by Euro-ISDN

The integrity of the data communicated is ensured by the Euro-ISDN, using a connection oriented transmission path with recovery of information attempted, if the exchange is interrupted. The meaning of "interrupted" includes, but is not limited to, loss of transmission path, alteration of information or loss of information.

3.4 Encryption

Encryption of data takes place after compression and is incorporated in the same way as the compression of binary data blocks (Fig.2). This scheme makes sense for two reasons [5]:

- Cryptanalysis relies on exploiting redundancies in the plaintext; compressing a file before encryption reduces these redundancies.
- Encryption is time-consuming; compressing a file before encryption speeds up the entire process.

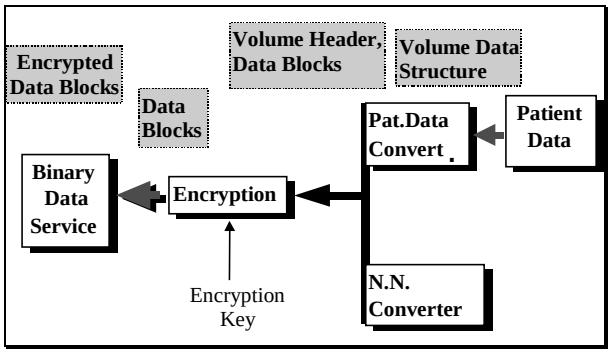

Fig. 2 Encryption - compression scheme

For the encryption of data over the LAN-to-LAN connection, a symmetric algorithm should be used, providing a high speed of encryption [6]. However, the choice of symmetric encryption rises the problem of key exchange, which is of high importance considering that communication patterns could be very complex, as every institution should be able to communicate securely with any other institution. This problem can be solved by using digital signature algorithms, such as RSA, to encrypt a session key that is then used from symmetric algorithms in a hybrid encryption scheme. Thus, the communication between two partners is a two - step procedure: a) the key is automatically generated by one partner, and then exchanged in secure conditions, using an asymmetric mechanism b) the key is used in a symmetric algorithm by both partners for the exchange of data.

3.5 Digital Signature

Non-repudiation and authentication of data are provided by the generation of an RSA signature, the computation of which for verification is not demanding. Every sending of data will be accompanied by an RSA signature, which proves the identity of the sender resulting to authentication of data, which is sent. Furthermore, signatures are securely stored preventing an attacker from illegally erasing a receipt, ensuring non-repudiation.

4 Conclusion

The secure communication among users of a telematics system for virtual simulation and treatment planning in clinical radio-oncology is provided over the LAN by backups and an access control system, with a log-in procedure and granting of rights of every group of users. Furthermore, on the LAN-to-LAN connection the integrity of data communicated is ensured by the Euro-ISDN protocol, while encryption and digital signature mechanisms provide confidentiality, authenticity and non-repudiation.

Acknowledgements

This work has been supported by the European Commission, DG XIII under the VIRTUOSO project (HC 4024) of the Telematics Applications Programme.

References

[1] Telematics Applications Programme, Project VIRTUOSO, 1998-2000.

[2] ACR/NEMA: The digital image communication in medicine (DICOM 3.0 standard), Vol. 13, No. 905013, NEMA Washington D.C., 1994.

[3] European Telecommunications Standards Institute, Recommendation on Integrated Services Digital Network (ISDN); Attachments requirements for terminal equipment to connect to an ISDN using ISDN basic access, 1995.

[4] INFOSEC Programme, Project S2304 THIS (Trusted Health Information Systems), CEC DG XIII/B, 1994.

[5] B. Schneier, *Applied Cryptography Second Edition: protocols, algorithms, and source code in C*, John Wiley & Sons Inc., 1996.

[6] P. Down, J. McHenry, Network Security: It's Time to Take it Seriously, *IEEE Computer*, Vol. 31, No. 9, 1998, pp. 24-28.