SECURITY IN HEALTH CARE: AN OVERVIEW

L. VORWERK, C. MEINEL, *Institute for Telematics, Bahnhofstrasse 30-32, D-54292 Trier, Germany*

SUMMARY

This paper describes standards which seek to integrate security, such as authentication and encryption, into the domain of health care. It also proposes several concepts according to these standards. There are two standards which have been developed in the USA. One of these has found acceptance from software developers in Germany. This standard, called DICOM (digital imaging and communication in medicine) [NEM96], is a modular and is often misunderstood. There are two security enhancements of DICOM which are under development. Therefore, a concept, [VLM00], was proposed that uses several definitions of the standard to construct a secure system for the management of patient data. An editor was implemented to integrate textual reports with images. Finally, a concept was developed that describes how to combine encryption and compression in order to make image processing faster.

INTRODUCTION

There are many approaches to guarantee security in health care. Several of them are proprietary, some are standards. Two of these standards are HIPAA (Health Insurance Portability and Accountability Act) [HIP98] and DICOM. They will be described now. The HIPAA, which was issued by the American Congress in 1996, aims at designating a new, comprehensive standard defining normative security requirements to be fulfilled for the communication between partners in health care and for the transfer of health-information data between parties of the health sector. The origin and background of this act lies in the fact that no recognized single standard exists, in which all components of security that are crucial in order to guarantee confidentially of health information is integrated. DICOM has two supplements which define how to integrate security (encryption, decryption, digital signatures, authentication) into DICOM. However, in the case of encryption and decryption, these definitions are not yet sufficient..

This presentation concentrates on the Institute for Telematics' development of concepts and software of the in the areas DICOM, security and image processing.

MATERIALS

The first element to be used is a multimedia-editor that conforms to DICOM [Vor98], [GVJ99], [VM00]. In order to understand how a multimedia-editor for radiology works, we need to have information about some of its inner details. The editor has a login mechanism and an option to freeze reports, so that no modifications may be

performed. Two features lead to security aspects like authentication and digital signatures. Programming languages used for the implementation of the editor are JAVA, for the visual construction of the DICOM reports and for the user interface, and C and C++ and a DICOM toolkit, to produce the DICOM conform reports saved in a file. Operating systems are either Linux, Windows NT/9x or Solaris. The editor works with SR (structured reporting) [GVJ98], [SR97]. It is important to consider the fact that reports must be updated to the new definition of SR. The reports produced by the editor may be stored together with the images in a PACS. A PACS is a picture archiving and communication system which is used for storing digital images. The final aim is to create a HIPACS (hospital integrated picture archiving system). A major feature of a high quality PACS is the degree of security which can be achieved by encryption. However, encryption and decryption have yet to be standardized . The DICOM standard (digital imaging and communication in medicine) possesses a supplement called SR which is used for encryption [VLM00] and which allows the definition of private coding schemes. Different coding schemes can be used for encryption and decryption and to connect several databases. The major feature of the intranet/internet-based PACS [VKM00], which was created at the Institute for Telematics, the fact that its components are distributed onto three separate computers. Interaction between the three computers takes place via secure connections. The data can either be sent encoded with the raw data, or separated from it. Thus, the separation of the components onto three independent, but still connected, computers results in a high degree of security. The digital images of a PACS have to be encrypted in several situations. The encryption algorithms slow the transmission speed if applied on the large amount of data contained in a digital image. Due to this, a solution for this problem is presented. An advanced way of dealing with large amounts of data is wavelets. Wavelets compress data. They allow a more flexible definition about which data is to be included and which is to be left out. The approach [VEM00] discussed here aims at combining the use of wavelets for image compression and, also, to use wavelet-transform for integrating encryption into the process. Other methods for a secure transfer of data are available. In [VLM00a] a method is described which uses TLS (transport layer security) to transfer confidential data between two locations. Here, an encrypted connection of two locations is used by using the programming language JAVA.

By using both techniques described above, together with the multimedia-editor, a separate transfer of image data and patient data is possible. The TLS-connection is used to transport the structured information (patient data, coordinates, DICOM-headers and so on) and the combined compression-encryption method is used to transfer the images that belong to the structural information.

The elements used here are:

the Standards HIPAA and DICOM;

DICOM supplements: Structured Reporting and the security enhancements;

the definition of wavelet compression:

the programming languages C/C++ and JAVA to implement the multimedia-editor and

a test application for the concept of the integration of security into wavelet compression as well as a test application for the TLS-protocol.

METHODS

The methods applied were taken from an existing definition, such as wavelet compression, the structured reporting supplement of DICOM, the master thesis of the DICOM conform multimedia editor or HIPAA. The definition is extended in the first three cases or evaluated, in order to use it in a special environment, as in the last case of HIPAA.

RESULTS

Obviously, the proposal for a secure HIPACS inspired the DICOM Workgroups during the development of the security enhancements and during the structured reporting supplement.

CONCLUSION

In case of the proposal for a construction of a secure HIPACS, this proposal must be considered as an alternative to the security enhancements. This concept, together with the multimedia-editor, the TLS-application, and the wavelet-encryption method, forms a system which is modular on the one side and multifunctional on the other .

REFERENCES

[GVJ98] S. von Gehlen, L. Vorwerk, P. Jensch, "Digitale Befunderhebung auf der Basis des DICOM Supplement Structured Reporting" in der Radiologie, in Biomedizinische Technik, Band 43 – Ergänzungsband 1, pp.46-47, 1998.

[VEM00] L. Vorwerk, T. Engel, C. Meinel, A Proposal for a Combination of Compression and Encryption, VCIP 2000, Visual Communications and Image Processing, K. N. Ngan, T. Sikora, M-T Sun, 694-702, SPIE, Vol. 4067, Perth, 2000.

[VLM00] L. Vorwerk, F. Losemann, T. Engel, C. Meinel, Constructing a secure HIPACS with Sturctured Reporting, MI 2000, Medical Imaging, G. J. Blaine, E. L. Siegel, SPIE, Vol. 3980, San Diego, 2000.

[VM00] A multimedia editor for making findings in radiology, CBMS (Computer based medical systems), Lutz Vorwerk, Ch. Meinel, 2000

[GVJ99] S. von Gehlen, L. Vorwerk, M. Eichelberg, P. Jensch, A multimedia editor for radiological reports based on the DICOM Supplement Structured Reporting, CARS `99, Computer Assisted Radiology and Surgery, H.U. Lemke, M.W. Vannier, K. Inamura and A.G. Farman, 438-442, Elsevier, Paris, 1999.

[Vor98] Lutz Vorwerk, Entwicklung eines Multimedia-Editors für die Befunderhebung in der Radiologie auf der Basis des DICOM Supplement Structured Reporting, (Master Thesis), Carl von Ossietzky Universität Oldenburg, November 1998.

[NEM96] *Digital Imaging and Communications in Medicine*, Teil 1{6. NEMA Standards Publication PS3.X, 1996.

[SR97] *Digital Imaging and Communications in Medicine (DICOM), Supplement 23: Structured Reporting (*Draft for Public Comment*)*, Supplement 23, Version 0.90-7 to NEMA PS 3.3, PS 3.4 and PS 3.6, 1997. Dr. Dean Bidgood and Ms Karen Kulda, NEMA-ACR and others.

[HIP98] Federal Register**,** Vol. 63, No. 155 , Part III, Department of Health and Human Services, Office of the Secretary, 45 CFR Part 142, Security and Electronic Signature Standards; Proposed Rule,1998.

[VKM00] L. Vorwerk, S. Khludov, C. Meinel, Concept for increased security for internet/intranet - based administration of patient data, WSCG 2000, Winter School of Computergraphics, V. Skala, ISBN: 80-7082-614-6, 124-129, University of West Bohemia Plzen, 2000.