MEDINFO 98
B. Cesnik et al. (Eds)
Amsterdam: IOS Press

"THE ELECTRONIC WARDENî Management of the Data Security Access in a Heterogeneous University Hospital Environment in Belgium.

C. Piret[a], F.H. Roger France[b], D. Clae[c],F. Dubr[d],

[a]*Service Informatique Hospitalier (SIH)*
[b]*Centre for Medical Informatics (CIM)*
[c]*Service Informatique Hospitalier (SIH)*
[d]*Service Informatique Hospitalier (SIH)*

Abstract

A very flexible software system called « Electronic Warden » has been developed. It is based on a « client/server » architecture. It controls and manages the access right of the complex and heterogeneous data computer system at St Luc Hospital in Brussels. The electronic warden is independent of the other software applications of the hospital and is connected to them through API'S. The physical access is managed with the use of smart card and allows the electronic signature. The management of the users and their accesses to the data is run in a centralised or a decentralised way which allows a lot of flexibility.

1. Problem description

Saint-Luc University Hospital has set up a series of coherent measures aimed at ensuring computer security.

Those measures have been developed in order to comply with the rules set by the Belgian legislation (2) as well as with the European directives (3).

In a previous article "Development of a coherent policy of Security - Confidentiality in a heterogeneous University hospital environment in Belgium (1)" we described the whole policy which had been set up.

In this article we will more specifically describe the computer system which has been developed as part of it. The Electronic Warden is a real access guardian for all computer applications within the hospital. The originality of the system lies in the global perspective of management of all accesses to the hospital computer applications and in its flexibility which enables to characterise individually each data access for each user while the daily management can be decentralised.

2. Environment

Saint-Luc University Hospital opened in 1976 in the southern part of Brussels. Its present volume activity is as follows : 30.000 patients hospitalised per year (900 beds), 300.000 outpatients per year and an average of 120 emergencies per day. It is a general hospital (medicine, surgery, gynaecology, obstetrics, paediatrics, medical imagery, ...) with high technology sectors (kidney - heart - liver transplants, laparoscopic surgery, intensive care ...) associated with a great number of research laboratories and educational activities.

The computer system is very heterogeneous. As a legacy of the past, there is a central data processing system composed along traditional lines : IBM ES 9000, AS 400 ; principally focused on administrative and accounting activities as well as personnel management (Payroll).At the level of medical activities, a heterogeneous collection of servers (NOVELL, UNIX, VAX VMS), gather medical protocols, laboratory results and uniform medical record summaries (MRS). In principle, these servers are, from the outset, completely independent form the central computer system and are developed, on an autonomous basis, by the different medical departments.The whole represents more than 400 terminals and 1.000 PCs spread on the site. The architecture of the networks makes use of a topology blending Ethernet and Token Ring, but evolves towards Fast Ethernet Switching.

3. The basis of the Security - Confidentiality Policy.

As the computer system is composed of a complex set of heterogeneous hardware, software and databases (SQL, Sybase, AS400, Dataflex, ...) a selection has been made of so-called "critical" applications, i.e. applications dealing with medical data of a personal nature (laboratory results, medical correspondence, surgical and technical protocols,).For those critical applications, a computer system has been set up allowing to sort out information in relation to access conditions for each person. Health care data have to be dynamically sorted out and distributed to the different medical departments staff members who are authenticated to handle concretely the authorised accesses benefiting the patients placed under their responsibility.This control is based on an application allowing to make up a complete chart of all the users entitled to access to the strategic computer applications. This form of control presents a dissuasive character but remains insufficient for critical applications in the medical sector.The implementation of this system of management for the existing network has permitted a restrictive policy to be developed, based on the individualisation of each access and by making responsible each requester of access. But it is only a static control.This point is explained in a previous article. (1)

The Electronic Warden

Principles

In order to improve dynamically the security systems described in 3, Saint-Luc wanted to build up an active control computer tool. This new tool was devised according to the following principles [4] [5].

1. The list of all known users of the computer systems had to be tightly linked to the personnel file. This list must therefore allow us to have at our disposal the information on the beginning and the end of contracts as well as the different appointments of the staff.
2. All the critical computer treatments which have to be submitted to access control must be known and managed dynamically.
3. A policy of security is decided at the Institution's Security Committee level. The consequences of its decisions must be passed on very rapidly.
4. A strict follow-up treatment (logfile) of all the accesses must be possible at any moment when requests demand so.
5. A dynamic access control must be set up based on a control of the computer treatments. The controls will therefore not be based on a classification of data fields. However, through access restrictions we can control the user-data link, for example : such doctor may only have access to data related to his/her own patients.
6. A management of the users' rights must be supported by a policy of centralised security even if a certain number of daily management actions can be decentralised to other people in charge.
7. The login rights on the data bases and the accesses to different objects in the databases must be automatically passed on the production servers. This work must be relatively transparent for the managers of the users' rights of access.

The Warden was developed on a client-server architecture (using SQL Windows with a Sybase relational data base). Starting from this very flexible type of architecture, we have developed a very reliable access system based on the principle that each member of the hospital staff corresponds to a function profile to which access rights are allocated for all or a part of the data arranged in categories

Description

The Warden is an information system which must allow the management and the control of access rights for applications for all the users of the different computer systems within the hospital. The control is meant to check any access first and later to allow to verify who accessed to what.The computer Warden is a module independent of the other applications of the hospital. It is connected to them through specific API's. The term "Warden" refers to the whole system or to one or another of its components according to the context.The first motivation of the Warden is to guarantee the respect of the patients' private life (and the hospital staff's) in conformity with the 8/12/92 law " relating to the protection of private life regarding the treatment of personal data " (2) However, the Warden can be used to limit the access to applications for other reasons than data confidentiality, for efficiency reasons for example.The access to the applications is managed, not via passwords, but via the use of smart cards with the following characteristics :

- personal card used for other purposes (restaurant, parking, payments, access to office)
- the connection to the computer application can only be obtained by the physical presence of the card in the scanner.

Practically, this system is composed of five distinct elements (picture 1).

1. A database is built to stock all the information concerning the computer processing, the users, their rights on the processing and the result of the tracking of the users' accesses (Security Database) :"hardware control", posts, cards,time-out,critical events,communication to critical applications ;
2. A Warden application, permanently open on the client post, which carries out the identification of the users and offers security services to other applications, management of all the databases, access and request logging ;
3. An Administration of the Security application (Security Administration) which allows to update the users' rights:management of the rights allowing to update the security databases.

   The person in charge of the Computer Security defines all the rights :

   - description of the structures of the applications (definition of the modules, of the DB objects) ;
   - definition of the users (Userids generation, personnel and DB's links) ;
   - security rules ;
   - definition of the security profiles (users' cards).
4. An edition module for access rights and logins for all data bases.

A class of access functions to databases has been developed to allow to filter transparently SQL requests launched by the computer applications.

Development of a secured application

Basic concepts

To develop a secured application consists in writing down a program :

- which uses the functions offered by the Warden. These functions are found in a DLL ;
- whose treatment entry points are carried out by functions interpreting the information transmitted by the Warden ;
- whose developer defines the criteria by which control can be ensured if it is required.

After the development of his application the programmer or the head of project will have to introduce the characteristics of the new processing inside the Warden database through the Security Administration application. Then, this new processing will be allocated to one or several groups of users. During the allocation of the new processing to a group of users the security manager can precise the security restrictions that will have to be respected as part of this allocation.The new application is then installed on the different client posts and at that moment all the authorised users will have access to it.We can use any programming language provided that it is possible to call functions from a DLL and to receive messages. Such is the case for C, SQL Windows, Visual Basic, Delphi, Forté, ...

Today the Warden has been implemented in DOS - Windows 3.11 and in Windows NT 4.0 environments. It is also possible to write down a C program which uses the Warden basic functions in another exploitation system (Unix, for instance). It is indeed possible as the DLL source code is portable and as only certain parts of the code are specific to Windows.

Users

To facilitate the security management the users are merged within different *groups*. A single user may belong to more than one group. When a right of access is allocated to a certain group, all users belonging to that group may benefit from it. We may also allocate rights individually to a specific user.A user may only have access to the processing (applications, modules or functions) for which he/she has a right of access. A right of access to processing may be submitted to constraints in order to limit the user's field of action within that processing.The constraints are formed by combining different restrictions with each other. The restrictions are classified according to different criteria : place of access, type of operation on the data, ...

Examples of restrictions:

- For reference use only
- For valid data only
- For non confidential data only
- For the patients' data only
- From a 21 Care Unit Station only.

Examples of constraints based on the above restrictions:

- His/her department's non confidential data only
- For reference use of his/her patients' valid data only
- From a 21 Care Unit Station only.

From then on, three scenarios can arise :

- Unlimited access of right.

  No control affects the treatment

  Right of access limited by one constraint.

  Alloperationswithinthetreatmentareaffectedbytheconstraint.

  Right of access limited by several constraints.

  At least one of the constraints must respected.

  For example, if we consider a right of access submitted to the three constraints mentioned above, all data may be reached provided that the access is made from a 21 Care Unit Station

Practical implementation

The Electronic Warden is currently under production for an application of computerised pharmaceutical prescriptions as well as for the computerised management of hospital care. The access by smart card allows doctors to use an electronic signature[6]. In addition, doctors have only access to their own patients' data, while nurses have access to data reserved for nurses only and related to their own care unit.A large number of different computer applications such as lab results, the Electronic Patient Record, appointments, the care units management, ... are or will be accessible through the Electronic Warden.The management of the access rights to the different applications can be run in a decentralised way by the different groups concerned. For example, the laboratories, the care unit, although a general control is always planned at the highest level.Eventually, all the hospital computer accesses will be treated through this system.

Conclusion

We have developed a very flexible system, based on a client-server / relational database architecture, of access control and management, for all the users of the different computer systems in the Hospital.The Electronic Warden is independent of the other computer applications in the hospital, to which it is connected through API's.The management of the users and their accesses to the data is run dynamically, both in a centralised and decentralised way. It allows to link individual rights to circumstances with a lot of flexibility.Finally, we must underline the fact that to ensure the private and untransferable character of the Smart Cards, they can also give access to personal data (salaries).

References

[1] Development of a coherent policy of security-confidentiality in a heterogeneous University environment in Belgium (C. Piret - F.H. Roger France - F. Pirard / MEDICAL INFORMATICS EUROPE 96 Copenhagen) J. Brender et al. (Eds) IOS Press, 1996 p 951 - 956.

[2] Le Moniteur Belge.Belgian law of 08.12.1992 relative to the protection of private life regarding data processing of a personal nature.

[3] SEISMED Consortium Data Security for Healthcare (3 volumes) IOS Press, 31-32-33, 1996.

[4] Proceedings of the IAMIA Workinggroup 4 - Working Conference Kobe Osaka - november 1997.

[5] Management de la sécurité des systèmes d'information J. Gonik AFNOR. - 1996 France.

[6] Arguments en faveur de la reconnaissance de la valeur juridique de la signature électronique. F. De Meyer et Al - Informatique et Santé 1998 (8) : 23-35 - Springer - Verlag France.