View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repositório do Instituto Politécnico de Castelo Branco

WEB-BASED ACCESS CONTROL SYSTEM

ANA TEIXEIRA, CRISTINA SANTOS, FERNANDO RIBEIRO, EURICO LOPES

Departamento de Informática, Escola Superior de Tecnologia do Instituto Politécnico de Castelo Branco
Av do Empresário, 6000-767 Castelo Branco, PORTUGAL
E-mail: {ateixeira, csantos, fribeiro, eurico}@est.ipcb.pt

This article describes a web-based system to control and manage the access to the ESTCB, which it is under development as a student's final project. Beyond an important pedagogical and technological value, we believe that this work is an important step towards offering strong and efficient security management for access control systems. We make use of standard technologies in use on the Web, to make an effective campus-wide security system. The system management and configuration, the consultation of access information for schedules, users, spaces, among others, will be carried out through the Internet. The proposed model is based on the use of two data nets: a CAN field bus to which are connected magnetic cards readers, door locks and sensors of each access place and the Ethernet that establishes connection between different CAN field bus and servers, which contain information about users and access rules.

1 Introduction

The fundamental objective of any access control system is to protect system resources against inappropriate or undesired user access [1].

The World Wide Web (WWW) technology has been widely used to synthesize diverse systems with great effect in web environments. In this article we propose an approach to access control systems, which will bring about a successful marriage of the web and roles of individual users [2]. We propose an architecture for making an effective campus-wide security system. In order to do so, we make use of standard technologies in use on the web. A magnetic card is used as an authorization device for user authentication. Authentication and authorization are two essential functions of access control systems: authentication is the means of verifying the identity of a user, and authorization is the means of determining whether the user is permitted access [3].

To provide a high quality of protection the access control technique must be directly integrated with the systems services, and must be able to support a wide variety of security system requirements. To be acceptable to users, it must not impose a significant performance overhead. A technique that meets these requirements would be of the greatest overall benefit to users [4].

Our proposed model is based on the use of two data nets: a Controller Area Network (CAN) field bus [5], to which are connected magnetic cards readers, door locks and sensors of each access place; and the Ethernet that establishes connection among different CAN field buses and servers that contains information about users and access roles.

This article is organized as follows: goals to achieve with the overall system, the architecture model, web technology integration, functionalities and conclusion.

2 Goals to Achieve

In agreement with the intended levels of security and considering the cost/benefit relation we opted to use magnetic cards. The magnetic card is a portable device that all users, students and staff, carry out and is also an identity card. This card has an acceptable level of security to be used in the generality of the installations. Thus, on a first phase the access control will be based on the magnetic cards, but it must be flexible enough to allow integration of different types of access control equipment, namely, when the installations need higher standards of security.

The system's main requirements are:

1. to be modular and allow its adaptation to different installations;
2. to allow its management is made through the Internet;
3. to allow consultations of access by schedules, users, access history and

4. to guarantee the information security between access places and the central system.

3 Proposed Model

Figure 1 shows the proposed architecture to achieve the previous goals. Main components are:

1. WWW server: manages the Internet/Ethernet interface to the system and has been implemented in a dedicated Windows NT server. It uses Professional Home Page (PHP) technology to generate dynamic HTML pages according to the database's information.
2. CAN field bus: is responsible for the transmission of the information collected from the magnetic cards readers to the database. It is also responsible for the transmission of the information needed to operate the door opening mechanisms when the access is authorized.
3. Access server: responsible for controlling all communications through the CAN field bus. Receives information on the existing accesses and stores it in the database. It is also responsible for placing the information in the CAN field bus in order to allow access to each one of the spaces.
4. System's database: contains information about the system's users and access history, as well the roles based access control about access authorizations. It is currently implemented using Microsoft SQL DBMS.

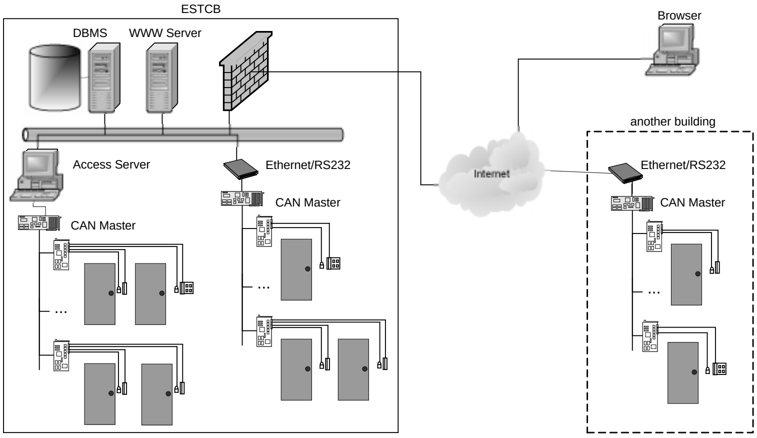


Figure 1. System's architecture.

The CAN field bus provides the system with high reliability, great capacity to support errors and is also inexpensive. For higher distances an Ethernet/RS232 bridge is used to link the CAN field bus.

Although the magnetic card provides adequate security in agreement with the installations to be protected in some spaces it can be necessary to increase the security level. To obtain this, a code can be associated with each magnetic card.

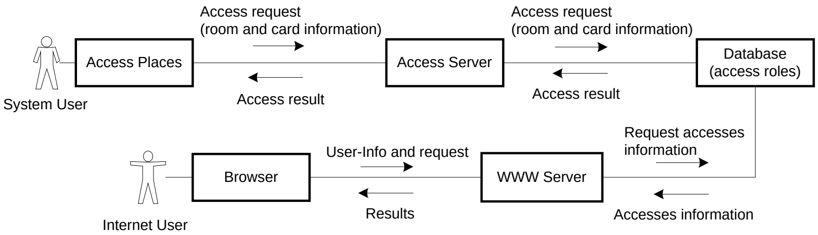


Figure 2. Proposed Model.

4 Web Technologies

Using C++ we developed the application that establishes the serial communication between the CAN Master board and data provided from magnetic card readers, to the database server.

All system information is stored in a SQL Server database. This database contains all the information about access roles and users as well as a description of accesses to each one of the spaces.

Using dynamic HTML pages, a user manage the system information. PHP is used to interface with the database. It is the server that transforms scripts into HTML making possible the access to the system by any browser. As a web server we use IIS (Internet Information Server) which is integrated in Windows NT.

The access monitoring in real time is implemented in Java.

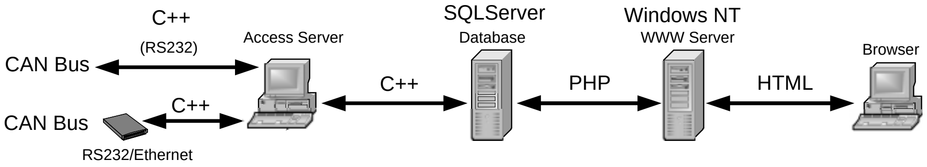


Figure 3. Web Technologies.

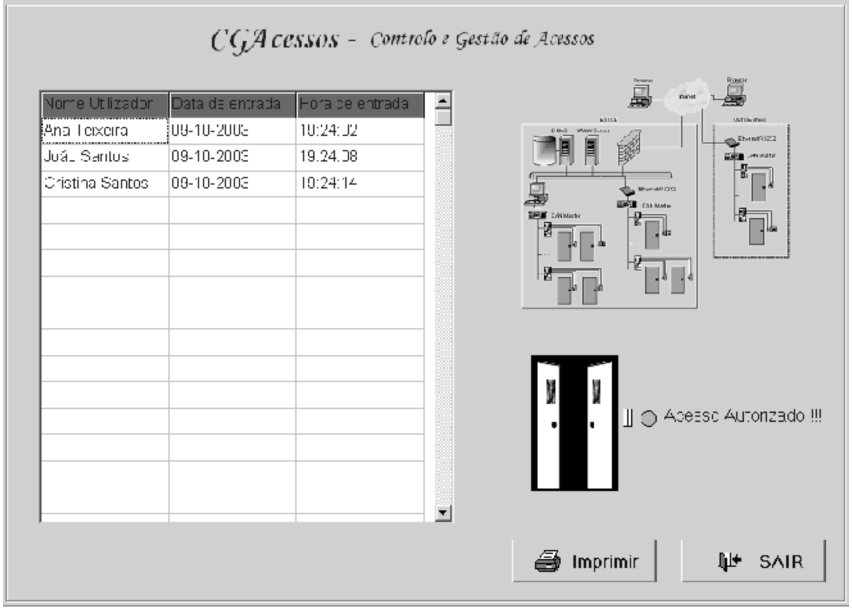
5 Some Functionalities

Using a browser a user can manage all the system's information. The system accepts two different levels of users: administrators that have full access for all information and guest that have some access constraints.

Although the system is still in a test phase it is already possible to present some results and to visualize some of its functionalities. Operations like eliminate users or insert news users and its permissions to accede to each space are easily realizable using a browser. The search for customized information about accesses is also possible.

Another interesting feature is the access monitoring in real time, which allows each time someone tries to access a space, information about that to be automatically modified in the browser, thus allowing the monitoring of several access or attempts of access.

Figure 4 shows the application that allows us the accesses monitoring in real time of each one of the spaces.



CGAcessos - Controlo e Gestão de Acessos

Nome Utilizador	Data de entrada	Hora de entrada
Ana Teixeira	09-10-2003	10:24:02
João Santos	09-10-2003	19.24.08
Cristina Santos	09-10-2003	10:24:14

○ Acesso Autorizado !!!

Figure 4. Real time monitoring

Some situations like locking, or unlocking, all doors from a remote place by an authorized user are also considered.

6 Conclusions

In a world each time more web dependent this application allows remote configuration and monitoring of everything that is related with the protected spaces. All the information is stored in database to allow statistical analyses.

We believe that our contribution is an important step towards offering strong and efficient security management for access control systems.

The proposed system provides a global form to carry out access control and management to the ESTCB campus in an inexpensive way using CAN field bus and the Intranet network.

References

1. David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli: Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security, Vol. 4. ACM Press, New York (2001).
2. Joon S. Park, Ravi Sandhu, Gail-Joon Ahn: Role-based access control on the web, ACM Transactions on Information and System Security, Vol. 4. ACM Press, New York (2001) pp. 37-71.
3. Richard Au, Mark Looi, Paul Ashley: Cross-Domain One-Shot Authorization using Smart Cards, ACM Special Interest Group on Security, Audit, and Control, ACM Press, New York (2002).
4. Stephen Smalley: Which Operating System Access Control Technique Will Provide the Greatest Overall Benefit to Users?, Proceedings of the Sixth ACM Symposium on Access control models and technologies, ACM Press, New York (2001).
5. Wolfhard Lawrenz, W. Lawrenz: Can System Engineering: From Theory to Practical Applications, 1st ed., Springer-Verlag, New York (1997).