Distributed system for access control to physical resources based on qualifications

DANIELA CRISTEA[1,2], OCTAVIAN PROSTEAN[1], THOMAS MUSCHALIK[2]
OVIDIU TIRIAN[3]
[1]Department of automatic and informatics
[3]Department of Electrotechnical Engineering and Industrial Informatics
"Politechnica" University of Timisoara
5 Revolutiei Street, Hunedoara
ROMANIA
[2]NWCON Technology Consulting GmbH
GERMANY
anadaniela05@yahoo.com, octavian.prostean@aut.upt.ro, t.muschalik@nw-con.eu, ovidiu.tirian@fih.upt.ro

Abstract: - This paperwork presents a distributed system required to implement a new method for the access control to physical resources, based on qualifications. It's a controlled access mechanism to be used by the employees of a company to access the inputs of certain machines, based on the qualifications (abilities) they dispose of. To get the qualifications required to apply this concept, the employees are offered modern learning possibilities.

Key-Words: - distributed system, authorization, access control, security, SAP NetWeaver platform, server

1 Introduction

In nowadays society, the computer system attacks are real threats, and terms as: *hacker, SPAM, phising, cyberterorism* are heard very often.

The experts in this field trigged a warning signal regarding the escalation of the cases when, through different techniques, someone goes for obtaining the authentication data of a certain entity (e.g. person, system), in order to abuse of its authority or, exploring the weaknesses of a system, to realize different types of attacks. The security lacks provoke important damages, situations about what we can often read on the first page of the world's well-known newspapers.

According to a statistic performed by CSI [1] based on the interviews with 144 organizations that agreed to offer information in this respect, the damages due to various security problems (e.g. viruses, unauthorized access to the systems) amounted, in 2008, approx. $288.618 per interviewed entity. The possible attackers of a system can be not only the hackers, criminal organizations, etc., but also the employees or former employees of a company that know very well the respective system. That's why the security should not be neglected, even in case of the functionalities created for the employees.

The protection of the information and the security of the access areas are daily necessities, being the reason why the controlled access to resources plays a more and more important role. These ones, along with other methods (e.g. Cryptography, Firewall), ensure that an entity can access only those information or only those physical resources for which it owns the adequate authorization. The controlled access to resources (physical and informational) is realized based on authentication and authorization. But, in the same time, we should take into account the fact that the usage of a solid authorization concept or an authentication method with high security degree doesn't necessarily mean the obtaining of a secure system. All these should be combined with the usage of other adequate security methods, with a secure programming able to avoid the vulnerabilities and to keep off the eventual attacks.

Hereunder, we present a model of access control to physical resources, based on qualifications that can be obtained through a learning process. The development of this model was imperative to grant to the employees of a company the possibility to access the inputs of certain machines (protected objects), according to the qualifications (abilities) they dispose of. To meet the requirements of our project, we have studied the design patterns existent in the field of patterns used for the access control to resources, but we found that none of the existent models fulfils completely the requirement of the project. That's why it was necessary to develop our own solution: the access to the inputs of certain

protected objects to be realized based on qualifications – QBAC [2]. The solution that grounded the controlled access method used in this paper has been inspired from the patterns [3]: Session, Extended Authorization, RBAC (Role Based Access Control), MBAC (Metadata Based Access Control) and Access Control to Physical Structures [4]. Besides a combination of their basic ideas, it was necessary to add our own elements, as the access based on qualifications or the addition of certain security elements for the physical level (e.g. to lock/unlock data about machines and employees).

The purpose of the present paper is to present the structure of the distributed system required to implement in this model its component elements, and the implementation modality.

2 The structure of the distributed system

Nowadays, the Internet plays a special role, offering to the employees either the access to secured networks (from distance) or the possibility to control, by Internet, certain industrial processes. The closed and simple systems where the access to resources is locally realized are not a common scenario anymore. One of the necessities brought by the globalization is the access to the resources of a corporation from all its centers spread in different parts of the world, the necessity to realize distributed industrial systems, the usage of standard protocols and more and more complex networks. This led to the extension of the industrial systems where, to ensure the security, the IT team should cooperate with the system engineers.

The structure of the distributed system for implementing the method of access control based on qualifications is presented in Fig. 1.

At the controllers' level, we used PLC (Programmable Logic Controller) of Siemens family. At this level, it is possible to connect those "n" eventual machines whose inputs can be accessed by the employees, based on the qualifications they dispose of. Each machine has its own RFID card reader that offers to the employees the possibility the login and logout. For programming and configure the PLC, we used "Step 7" software that offers some facilities, e.g. testing, diagnosis, on-line function to display all the used variables. "Step 7" disposes of three basic programming languages, to which it is possible to add more languages to extend its functionality.

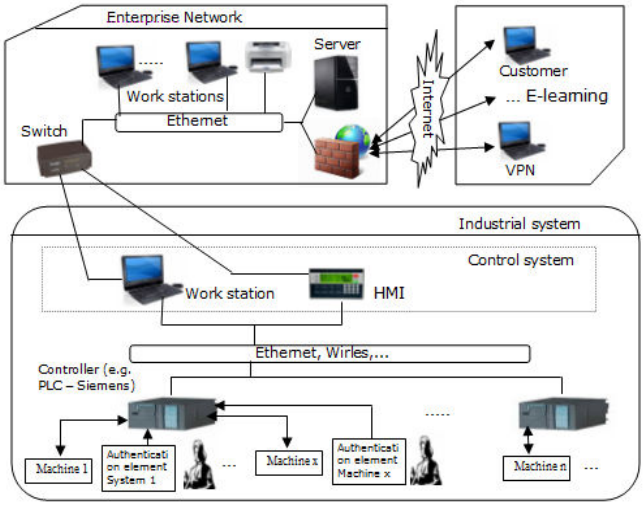

Fig.1 The structure of the distributed system for implementing the access control model based on qualifications

In the present project, we have mostly used the S7-SCL language (useful in case of complex algorithms), along with the FBD language.

All the development objects required for the controlled access method based on qualifications are created at the server level. For the server part, we chose the SAP NetWeaver platform [5] because it offers certain advantages, as follows:

- Large variety of modules that can be used
- Application Server ABAP and Application Server Java
- Portal through SAP NetWeaver Portal
- MVC (Model View Controller) support
- Easiness to work with Web Services and ActiveX

The creation of the employees' data, along with the data required for the learning process (e.g. courses, qualifications) has been realized by using the SAP HCM module [5] (Human Capital Management). Of a special importance are the data key of each employee (an identification number made of 8 digits that is also imprinted on the RFID identification cards) and the key of each qualification. For each machine, we created three qualifications: Installer, Operator and Tool_Setter. Then, we assigned to each qualification a number of inputs of the respective machine.

So, when the employee disposes of a qualification, he/she has the authorization to serve the respective inputs of the protected object. For each machine, an employee may dispose of multiple qualifications. In Fig. 2, we presented the Qualification catalogue of four test machines.

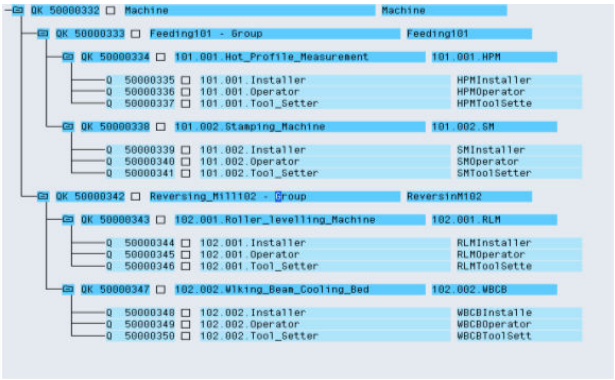

Fig. 2 Qualification Catalogue

In this project, the QBAC pattern has been combined with the RBAC pattern to offer modern learning possibilities (E-learning) to the employees, along with the possibility to make reservations for courses through the company portal, Fig. 3.

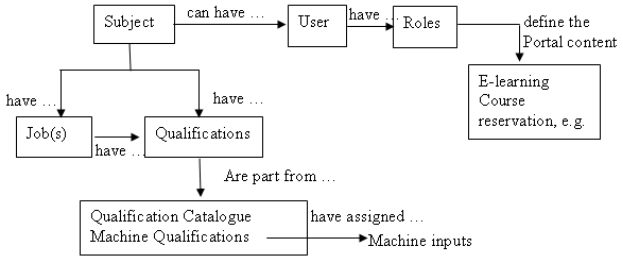

Fig. 3 Relation QBAC - RBAC

To realize the required functionalities, we created development objects, as follows:

- Relational database
- Classes and methods
- Access right exposed as Web Service
- Web Dynpro application [6] to manage the machine integration
- Portal object required to make reservations to a course or to perform E-learning.

In this paper, we are going to present only the structure of the database and the management application.

The scope of the database is to realize the connection between the machines (their inputs) and the database generated when creating data in the SAP HCM module. In Fig. 4, we present the part that integrates the machines in the controlled access process, the *Connection_with_human_resources* and *Conection_with_learning_solutions* tables, making the connection with the HCM data (the submodules Human Resources and Learning Solutions).

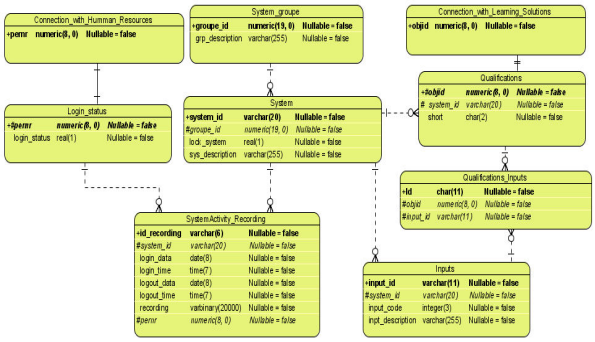

Fig. 4 The database required to integrate the machines in the controlled access method

The modality to implement the management application Web Dynpro (of the interface level) with the machines is presented in Fig. 5.

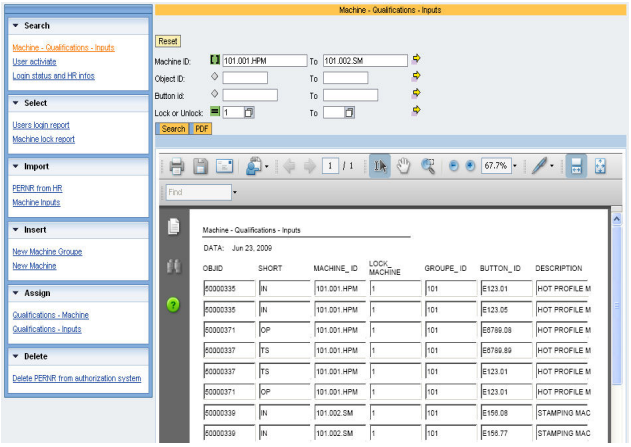

Fig. 5 Web Dynpro management application

From the basic functionalities, we mention only the possibility to create different reports in PDF format (to track the employees' activity) and the possibility to import the names and inputs of the machines from text files.

At the Work Station level in the area "Control system", it is realized the communication between PLC and server, having the possibility to access certain process values. In our project, we used a Web Service for the communication with the SAP NetWeaver platform. So, in a Visual Basic application, it is consumed the Web Service that are going to grant access right to an employee to the inputs of one of the protected objects. The access right obtained from the server will be transmitted encoded in an integer, from where it will be decoded at the PLC level. In the same Visual Basic application, it is used an ActiveX (client's OPC) meant to communicate with an OPC server. All these are schematically presented in Fig. 6.

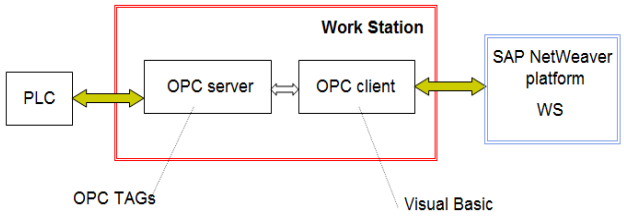

Fig. 6 Schematic representation of the communication PLC – server, through control Work station

So, by using Web Service, we will obtain data from the server anytime when an employee wants to login to one of the machines, and we will insert some values at the server level, e.g. the activity of a subject during the login period, date and time of logout, the machine where he was logged, etc. By using Web Service, we can also offer these data in case that certain machine is distributed outside the Ethernet.

Another possibility to communicate between server and PLC, through the control Work Station, is to use the ActiveX (client's OPC) directly in the ABAP coding, communicating in this way with the OPC server, to read and write data in PLC.

The other Work Stations located in the area "Enterprise network" are used to create all the development objects required at the server level, for the administrators of this model, for the company's employees that work in offices, etc.

The company's employees and the clients can access the server from the outside, through Internet. For example, a client can read about the company's offers, while an employee of the company can program, in the integration platform, by using the VPN connection.

3 Further research

The access control model presented in this paper has been implemented only one time, as prototype; further developments shall be made especially at the hardware level. The server level algorithms and the PLC are generalized created, for the "n" machine, but for testing at the hardware level we used only one test machine and one PLC Simatic S7-300, with the modules: RFID interface, Inputs, Outputs, Ethernet. In the same time, further developments shall be realized on the security part, where certain improvements are required, e.g. to secure the Web Service with digital signatures.

4 Conclusion

This paperwork describes the implementation method of the access control to physical resources, based on qualifications. The advantage of this model is not only the fact that the access to resources is realized based on qualifications, but also the followings:

- The integration of the qualifications in the authorization process helps us in the human resources process, too. So, we can easily answer to questions of this type: *What qualifications are missing to an employee to fulfill the plumber job at the machine x*?
- Combining QBAC with RBAC, the employees are offered modern learning modalities

In conclusion, if we look at the obtained results from the point of view of a distributed system, we can say that we obtained a system: transparent (the components are well combined, making a whole), open (it uses protocols and standards, flexible and easy to configure or add new components), relative secure (because the future developments shall cover certain lacks of the test variant). Regarding the Scalability and Concurrence, they are going to be tested in the next variant, when we will benefit of sufficient number of test machines.

References:

[1] Robert Richardson, CSI Director, 2008 - *CSI Computer Crime & Security Survey*, available online: http://www.cse.msstate.edu

[2] Cristea Daniela, Octavian Prostean, Thomas Muschalik and Tirian Ovidiu, *An access control pattern based on qualifications to grant access to physic resources*, The 3rd European DAAAM International Young Researchers´ and Scientists´ Conference 25-28th, Vienna, Austria 2009, ISBN 978-3-901509-70-4, pp. 1765 – 1766

[3] Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann and Peter Sommerland, *Security Patterns Integrating Security and Systems Engineering*, John Wiley & Sons, Ltd, 2006, ISBN: 0-470-85884-2.

[4] Fernandez, E.; Ballesteros, J.; Desouza-Doucet, A. & Larrondo-Petrie, D. (2007). *Security Patterns for Physical Access Control Systems*, in: Data and applications security XXI, Barker, k. & Ahn, G. (Eds), 259-274, Springer, ISBN: 978-3540735335, Germany

[5] Martin Raepple, *The Developer's Guide to SAP NetWeaver Security*, SAP Press, ISBN 978-1-59229-180-9

[6] Gellert Ulrich and Cristea Daniela, *Web Dynpro ABAP for Practitioners*, Springer, 2010, ISBN 978-3-642-11386-4